ITEM NO: 4

REPORT TO:	**STANDARDS COMMITTEE**
DATE:	8 October 2013
REPORTING OFFICER:	Wendy Poole – Head of Risk Management and Audit Services
SUBJECT:	**INFORMATION GOVERNANCE**
REPORT SUMMARY:	To highlight the proposed policies, procedures and protocols in relation to the delivery of the Information Governance Framework.
RECOMMENDATIONS:	The Standards Committee are recommended to (1) Support the approval and adoption of the Information Governance Framework by the council; (2) Agree consultation with Trade Unions and consideration by Audit Committee before recommending to Council.
FINANCIAL IMPLICATIONS: **(Authorised by Borough Treasurer))**	Non-compliance with the Data Protection Act 1998 can result in the Information Commissioners Officer imposing financial penalties up to £500,000.
LEGAL IMPLICATIONS: **(Authorised by Borough Solicitor)**	The report details the Information Governance Framework which the Council proposes to implement to ensure compliance with the Data Protection Act 1998 and minimise against the unauthorised disclosure of personal information.
RISK MANAGEMENT:	Information is a valuable asset and needs to be protected from loss, theft, misuse, inappropriate disclosure or corruption as privacy failures could be very damaging to the Council's reputation. The Framework recommended should ensure that the risk exposures for the Council are managed and mitigated in line with recommended best practice.
LINKS TO COMMUNITY PLAN:	Information Governance supports the individual operations which deliver the objectives within the community strategy and ensures that the public can have confidence in local government.
ACCESS TO INFORMATION:	**NON-CONFIDENTIAL** **This report does not contain information, which warrants its consideration in the absence of the Press or members of the public.**
REFERENCE DOCUMENTS:	The background papers can be obtained from the author of the report, Wendy Poole, Head of Risk Management and Audit Services by contacting: Telephone:0161 342 3846 e-mail: wendy.poole@tameside.gov.uk

1. INTRODUCTION

1.1 Information is a vital asset and needs to be protected. Information Governance is not a new concept as the Data Protection Act has been in place since 1998. The NHS has been governed by Information Governance for several years and several of our Directorates are involved with Information Sharing Protocols, Caldicott Guardians and Safe Haven Policies because of their partnership working. However, over the last few years new guidelines have placed the responsibility on Local Authorities to have corporate policies in place covering information governance.

1.2 In the last 12 months there have been a number of information security incidents across the UK. These have included the publishing of vulnerable children's welfare details on line, to a council employee sending details about an adopted child to the birth mother, and including details of the adoptive parents' home. The Information Commissioner himself has stated *"…Far too often in these cases, the councils do not appear to have acknowledged that the data they are handling is about real people, and often the more vulnerable members of society…."*. These incidents and the ICO's comment highlights the requirement for all public bodies to act to bolster public trust and confidence in the way personal information is handled and kept safe.

1.2 The Data Handling Review was published in June 2008, putting in place a set of mandatory measures for Central Government on protecting personal data. From this, the Local Government Association produced the Local Government Data Handling Guidelines detailing each of the measures that need to be in place for the successful protection of information. The 2008 guidelines have now been updated into the Local Public Services Data Handling Guidelines August 2012.

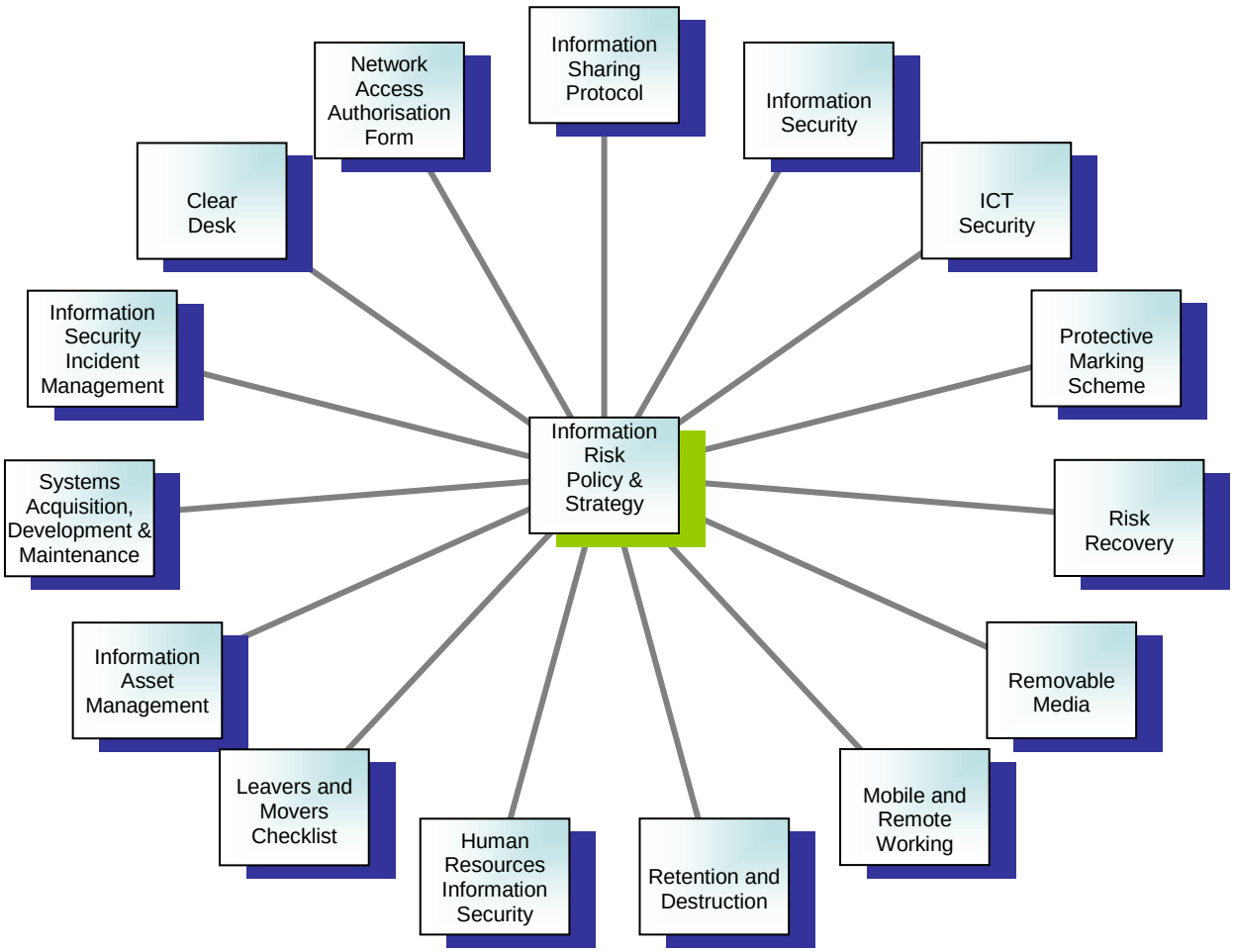
1.3 The 2012 Data Handling Guidelines are structured into five sections:-

- Policy;
- People;
- Places;
- Processes; and
- Procedures.

Under the People section one of the key recommendations is that a Senior Information Risk Owner (SIRO) is appointed who is accountable for risk management within the organisation. This role has been assigned to the Head of Risk Management and Audit Services who reports directly to the Executive Director of Finance and works in conjunction with the Executive Director of Governance.

1.4 Furthermore, the Information Commissioner's Office (ICO) has been granted powers to enforce the appropriate protection of information. The ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. They now have the authority to carry out assessments of organisations to ensure their processes follow good practice, along with the power to impose monetary penalty notices for breaches of the Data Protection Act 1998. Organisations may have to pay up to £500,000 as a monetary penalty for serious breaches.

1.5 To deliver the requirements placed upon the Council and ensure full compliance with the above guidelines an Information Governance Framework was produced, which incorporated a suite of new and existing policies and procedures. The requirements of the Data Handling Guidelines (2008 and 2012) have supported the structure and content of the Information Governance Framework. The Information Risk Management Framework below was first presented to the Executive Team in July 2010, together with the Information Risk Policy.



Tameside Information Risk Management Framework

2. CURRENT POSITION

2.1 A significant amount of work has been undertaken since then to produce the supporting documents and guidance that make up the framework. Wherever possible documents produced by the Records Management Society, National Archives, Information Commissioners Office and other LA's have been used as a starting point for new documents, as well as integrating existing policies where appropriate. As we have undertaken more research the framework has been updated and some of the original documents thought to be required have been merged together to limit the number of documents making up the framework.

2.2 The framework has also been renamed the Information Governance Framework taking the emphasis away from risk and giving it a broader remit as it is a system of control to ensure that we do the right things, in the right way, for the right people, in good time, and in a fair, open, honest and accountable way.

Revised Tameside Information Governance Framework

2.3 Since the introduction of the Data Protection Act 1998 employees have had a defined responsibility to handle personal information in a safe and secure way. The expectations and requirements placed on Council employees have grown, following the issue of the Data Handling Guidelines, the additional guidance issued by the ICO and the numerous publicised losses of very sensitive information.

2.4 The purpose of the framework is to support employees in adhering to the principles of the Data Protection Act whilst discharging their duties. By putting in place a system of controls to mitigate the risk exposures identified which should then prevent information breaches. The objective is to keep the Council, employees and the information subjects safe and prevent the ICO from issuing a monetary penalty (up to £500,000) or enforcement notice for non-compliance against the Council, but also potential individual fines or prosecutions against employees.

2.5 The Framework has been facilitated by the Risk and Insurance Team under the direction of the Head of Risk Management and Audit Services. A corporate Information Governance Group chaired by the Executive Director of Finance with members from ICT and Legal Services has been involved from the outset and contributed to the structure of the Framework and the supporting documents and procedures. Reports to both the Executive Team and the Senior Management Team have also helped to develop the framework.

2.6 Each document in the Framework is intended to give support and guidance on an identified subject, which could pose a risk whilst employees are discharging their duties. Also by integrating existing policies into the Framework, it is possible to build on already established obligations.

2.7 At the core of the Framework there are two documents the Information Governance Policy (IGP) and the Information Governance Conduct Policy (IGCP). The Conduct Policy is intended to direct employees to the documents they need to understand and the expectations placed on them by the Council, whilst handling personal/sensitive information in order that they can discharge the responsibilities placed on the Council by the Data Protection Act.

2.8 In addition to work on the documents and guidance relating to the Framework, work has also been undertaken in the following areas:-

- **Advice, Guidance and Consultation**
  Workshops and one to one training has taken place with employees in high risk areas to raise awareness of their obligations in relation to information security, whilst awaiting the implementation of the framework. Additionally the Information Risk Officer and the Risk and Insurance Manager have provided assistance to managers and employees regarding specific situations. They have also held consultation/engagement workshops with managers and employees around the implications of the documents to assess the practicality of the changes proposed. The feedback from these consultations was then incorporated into the documents.

- **Online E-Tutorial Training**
  An E-Tutorial was launched in September 2010 and completed by the majority of employees. This is now to be followed up with new and revised mandatory training through the AGMA Virtual College.

- **Training for non PC users designed and being delivered**
  An initial risk assessment was undertaken with Managers and Business Support Managers for all non PC users to determine their exposure to information risks resulting in several groups of employees being assessed as very low risk and therefore not requiring any training. A fact sheet and training material was developed and the training was provided to meet user requirements.

All of this additional support is necessary and will continue to be delivered to assist and support employees with their information governance responsibilities.

3. DOCUMENTS FOR CONSIDERATION

3.1 The revised Information Governance Framework has generated a number of new documents and has incorporated some existing policies, which provide support to the ethos of information governance. The Information Technology and Email Security Policy 2008 has been divided up into more focused smaller documents to signpost employees more directly. As the policy has been in place for many years a comparison table has been produced tracing each element of the 2008 Policy to the new framework documents. Details can be seen in **Appendix 1**. The following sections of the report give a brief overview of the various documents within the framework

3.2. **Information Governance Policy** - This is the overarching document, which details why the Council needs to protect information and the adopted Information Governance Framework. It outlines the purpose of the policy, the scope of cover and the responsibility for risk management and the expectations for protecting the Council's information assets from

threats. It also lists the key roles and responsibilities for managing information securely within the Council. **See Appendix 2.**

3.3 **Information Governance Conduct Policy** - This conduct policy outlines the expected behaviour, roles and responsibilities of employees regarding information governance and indicates the minimum relevant documents that employees are expected to read and understand to meet their responsibilities. It also indicates what the consequences are of contravening the requirements of this policy and the documents within the overall Information Governance Framework. As stated in the policy this may lead to disciplinary action and in cases where individuals have been negligent and not followed guidance and policies, legal action may be pursued not only by the Council but other regulatory bodies. **See Appendix 3.**

3.4 **ICT Security Policy** - This document sets out the responsibilities for using and securing the Council's hardware, software and networks. It is based on the content contained within the existing Information Technology and Email Security Policy – April 2008. It details the Council's rights and obligations, and outlines the consequences of using Council Technology in a harassing or abusive manner and the disciplinary implications of not complying with the policy. The communications and internet aspects have been separated out into a specific policy for clarity for employees. **See Appendix 4.**

3.5 **Email, Communications and Internet Acceptable Use Policy** - This policy has the same content as previously contained in the Information Technology and Email Security Policy. It sets out the expectations of individual's conduct and responsibilities when using the Council's email and Internet facilities, including business and personal use of email (including the personal use of Council and non-Council/personal email accounts). Work related and personal use of the internet (including websites accessed and transactions permitted for work or non-work purposes). It also explains what will happen if Council systems are used for harassment or abuse and the disciplinary implications of not complying with the policy. **See Appendix 5.**

3.6 **Social Media Responsible Conduct Policy** - This is an existing policy that has been incorporated into the Framework. This policy applies to all employees whilst participating in any on-line social media activity, whether privately or as part of their role with the Council. It sets out the standards of behaviour the Council expects of all its employees, when using social media services. The disciplinary implications of inappropriate posting on social media websites are explained. It also advises on using social media safely, legally and appropriately and points out that employees are personally liable for what they publish online. **See Appendix 6**.

3.7 **Protective Marking Scheme (ON HOLD)** - The Council's Protective Marking Scheme will be based on the Government Protective Marking Scheme. However, finalisation of the scheme is on hold whilst technological solutions to assist employees to comply with the requirements are assessed.

3.8 **Removable Media Protocol** - This protocol aims to ensure that the use of removable media is securely controlled. All those who have access to or use of removable media are responsible for the safety and security of the media and the information stored on them. Service areas are responsible for implementing this procedure and must monitor the use of removable media. The protocol explains the types of removable media that can be used and the security necessary for use. There is also an explanation of how to dispose of removable media securely. Loss of any unencrypted removable media could result in a potential breach of the Data Protection Act 1998 and subsequent disciplinary action for the employees involved. **See Appendix 7.**

3.9 **Mobile and Remote Working Protocol** - This protocol applies to any access or use outside of Council controlled premises of any ICT Council equipment including mobile telephones,

portable devices and static IT equipment. Employees are advised of their responsibility for the safety and security of portable devices and the information on them, issued to or used by them. Explanations of what physical security is required on the devices and how to use them in line with the Council policies and procedures are provided in this document. **See Appendix 8.**

3.10 **Retention and Disposal Guidelines/Schedule** - The schedule outlines the timescales involved for the retention and disposal of information held by the Council. The Retention and Disposal Guidelines will ensure that the information the Council holds is retained for only as long as it is needed to enable it to operate effectively. They also cover the correct disposal methods to be used. Working within the schedule will ensure the Council complies with legislation and the requirements of regulators. **See Appendix 9.**

3.11 **Access and Security Protocol** - This protocol is aimed at managers and indicates the steps required to ensure that access to Council information, information systems or ICT equipment is controlled. Access for employees needs to be restricted on a need to know basis and removed as soon as it is no longer required. The document also includes the Leavers and Movers Checklist, which is an aide memoire for Managers when a member of staff leaves or transfers to another area. As information is held in both paper and electronic format this procedure relates to both physical and technological access. **See Appendix 10**.

3.12 **Incident Reporting Procedure** - This procedure must be applied as soon as Council information or information systems are suspected to be, or are actually affected by an adverse event which is likely to lead to an Information Security Incident (ISI). All incidents, irrespective of scale, must be reported to ensure that a thorough understanding of what has occurred is recorded, to improve information handling procedures, the incident response process and any subsequent action that may be required. **See Appendix 11.**

3.13 **Secure Desk Procedure** - This procedure reduces the threat of a security breach as information should be kept out of sight. This procedure applies to all information of a personal, confidential or sensitive nature. It also covers any information that is accessed, viewed or stored within a shared space (i.e. main office, home or Touch Down Point). If non-compliance of this policy results in a breach of the Data Protection Act 1998, subsequent disciplinary action for the employee could arise. **See Appendix 12.**

3.14 **Personal Device Policy -** This policy states the acceptable ways to access Council systems on employee's personal devices. It outlines that by using a personal device to access the Council's systems and information an individual is accepting responsibility for the safeguarding of information viewed on that device and will be held accountable for any incidents which compromise the safety and security of the Council information they are utilising. Failure to adhere to this policy may lead to disciplinary action being taken and for more serious cases, where individuals have not followed guidance and policies, legal action. **See Appendix 13.**

3.15 **Information Asset Register** - A register now exists for each Directorate and details what information assets are held, who owns them and what format they are held in.

3.16 **The Golden Rules** - The Golden Rules briefly outline how to use information assets responsibly within the framework of the law. They ensure that employees understand the corporate policies with which they must comply. It signposts the mandatory corporate on-line training employees must undertake so they are aware of their responsibilities All employees must comply with the minimum corporate security standards set out in these rules which are based on the Council's Information Governance Framework and also follow any localised business specific data handling requirements. **See Appendix 14.**

3.17 **The Managers Checklist** - This checklist has been provided for Managers/Supervisors to enable them to identify the areas they should be considering on a regular basis to ensure

compliance with the Information Governance Framework. It can be used as many times as necessary to review changes. It also details the available resources to assist Managers/Supervisors in complying with the appropriate actions required. **See Appendix 15**.

3.18 **Information Sharing Protocol -** This protocol is the overarching document that outlines the responsibilities of employees when sharing information. It applies to all sharing of information, potentially internally and externally to the Council. Information Sharing or Processing Agreements will govern specific exchanges of information and will specify what information is to be shared, how it will be shared and for what purpose the information is required. Failure to comply with this protocol, when sharing information would constitute a breach of the Data Protection Act 1998 and could result in disciplinary action. **See Appendix 16**.

4. EMERGING ISSUES

4.1 It has become apparent during the creation of the above documents that to satisfy the requirements of the Data Protection Act, the Information Commissioners Office and best practice and mitigate the risk exposures facing the Council there may some impact on service delivery. Is it critical that the framework is practical and supported, as we would be heavily criticised by the ICO for introducing something that is ignored. Therefore every effort has been made to ensure that workable solutions have been recommended by consultation with senior managers and by learning from the enforcement actions issued by the ICO.

4.2 The introduction of the overall Framework does have potential disciplinary implications for employees. The procedures/guidelines/protocols are being recommended to support the public's expectations regarding the security of the information they provide to the Council. Also to provide a level of risk mitigation and protection for not only the Council, but individuals as well. As can be seen from the recent prosecution by the ICO, they will fine individuals.

News release: 15 August 2013

A probation officer who revealed a domestic abuse victim's new address to the alleged perpetrator has been fined £150 following a prosecution bought by the Information Commissioner's Office (ICO).

Victoria Idowu claimed that she provided the victim's full name, new address and date of birth, along with the details of the investigating officer, as she believed that the individual already knew this information and she was keen to avoid a case of mistaken identity.

The victim subsequently contacted the investigating officer on 6 January 2013 - the day the information was illegally provided - in a distressed state confirming that the perpetrator was now aware of their new address. The victim broke off all contact with the police and the other services involved, believing that they could no longer be trusted. The investigation against the alleged perpetrator was subsequently dropped.

Appearing at Camberwell Green Magistrates Court today, 39-year-old Victoria Idowu was prosecuted under section 55 of the Data Protection Act and fined £150 and ordered to pay a £20 victim surcharge and a £250 contribution towards costs.

Information Commissioner, Christopher Graham, said:

"This is the unpleasant but unremarkable face of data protection crime – not journalists, not lawyers, just individuals for whom the current sentencing regime holds no terror.

"Ms Idowu escaped with only a relatively minor penalty and no criminal record. The government must act now to introduce tougher penalties for individuals who illegally access and disclose personal information.

http://www.ico.org.uk/news/latest_news/2013/probation-officer-prosecuted-for-leaking-victims-details-to-alleged-culprit-15082013

4.3 Due to the constantly changing landscape of information governance both in terms of guidance and technologies all the framework documents will be kept under constant review to ensure they meet the needs of the business.

5. AWARENESS CAMPAIGN

5.1 A comprehensive communication, training and awareness strategy is being developed to ensure that the framework is successfully implemented and that messages are getting to and understood by the end users.

5.2 The communication strategy includes :-

- Articles in the Chief Executive's Brief and Wire;
- Roll out of the AGMA Data Protection E Learning Module;
- A poster campaign;
- Classroom 30 Minute awareness sessions;
- Written briefing notes provided to managers;
- Roll out of the AGMA Information Security E Learning Module
- Explicit referencing in the Induction Checklist;
- Reminders on the Bulletin Board;
- Requirement for employees to read the Information Governance Risk Policy and Conduct Policy; and
- Face to Face Training tailored to Service Area requests.

6. SERVICE AREA MONITORING AND REVIEW

6.1 A Temporary Information Risk Officer has been appointed and a programme of Data Protection reviews based around the IRM Checklist for Managers and the Golden Rules will be scheduled across all Directorates following implementation. It is envisaged that the reviews will be a mixture of interviews and surveys using 'Survey Monkey' and the learning from the reviews will be incorporated into future training and used to improve the information governance framework.

7. RECOMMENDATIONS

7.1 As set out at the front of the report.

APPENDIX 1

Content in 2008 Document	Description of content	Moved in IT Security Policy	Moved in Email/Internet Acceptable Use	Comments from IT
1 - Introduction	Purpose of the policy and what it covers	Section 1- Removed 1.1 *gain maximum benefit from email and the internet*	*1.1* Section 1 – 1.2 changed from *This policy sets out the Council's policy on using its computers and networks, including all devices such as telephones, mobile phones; faxes; printers, scanners and anything of an electronic nature otherwise referred to as information technology etc. This equipment is for clarity of understanding referred to throughout this policy as the Systems*, to, *This policy sets out the expectations of individual's conduct and responsibilities when using the Council's email and Internet facilities, including;* ➢ *Business and personal use of email (including the personal use of Council and non-Council/personal email accounts)* ➢ *Work related and personal use of the internet (including websites accessed and transactions permitted for work or non-work purposes)* ➢ *Business and personal use of social media (including the posting of information on social media sites whether related or unrelated to any Council business)*	

APPENDIX 1

Content in 2008 Document	Description of content	Moved in IT Security Policy	Moved in Email/Internet Acceptable Use	Comments from IT
2- User Responsibility	What users are responsible for with regards to equipment purchase/maintenance/security	Section 2 - Addition of insurance related paragraph		
3- Management of Data, Information and Software	Expectation on employees when managing data	Section 3 - see IT comments		3.1c (Data Protection - keeping data confidential) Added: *When sharing such information with third parties, checks should be made to ensure that third parties are registered as a data controller under the Data Protection Act 1998.* Per ICT Support and Maintenance Internal Audit; 29/09/2009; ref. 2.12.2.
4 - Authorised Business Use	Permissions for using equipment / systems. Expectation that all communications follow a corporate standard	Section 4 – see IT comments		4.2 (Authorised Business Use) Amended: *In order to ensure accountability in the use of the Systems, you must never use any ~~laptop or mobile phone~~ computing device without the permission of the main allocated user. ~~You must never use any computer when another user has logged into it unless you have the permission of that user or the Council's permission.~~* This amendment provides improved accountability. There is no reason why login information should be shared. In the event that information needs to be retrieved from (e.g.) a PC, IT can log in using an administrator's account to retrieve the data.

APPENDIX 1

Content in 2008 Document	Description of content	Moved in IT Security Policy	Moved in Email/Internet Acceptable Use	Comments from IT
5 - Unauthorised Use	Guide to things staff should never do	Section 5 - No change to wording		
6 - Passwords and Security	Guidance on maintaining password security	Section 6 - Added *For further guidance please refer to the ICT Service Portal for Password Guidance. Click here and type 'password' in the search box* Added: *For further information, please refer to the Removable Media Protocol.*		6 (Passwords and Security) 6.2 Amended: *It is the Council's policy that passwords should~~, where possible,~~ be changed at regular intervals. ~~Where possible you must change your selected passwords on a regular basis.~~ During the course of your employment you are likely to be responsible for creating some of your own passwords. When creating a password, you should not select a password that can easily be deduced by others; in particular, you should not use passwords which are easy to guess (e.g. the names of partner children or pets). It is advisable to ~~include a~~ use a mix of characters, e.g. 3 out of four of: upper or lower case alphabetic characters; numbers and symbols in each password.* Removed ambiguity and repetition. Per external audit guidance. 6 (Passwords and Security) Added: *6.5 When an employee leaves the Council, their access to computer systems and data must be deleted on the employee's last working day. It is the responsibility of the line manager to request access deletion via the ICT Service Desk. Similarly, HR must inform ICT*

APPENDIX 1

Content in 2008 Document	Description of content	Moved in IT Security Policy	Moved in Email/Internet Acceptable Use	Comments from IT
				Services when any staff members change jobs within the Council so that systems can be amended and the user's systems access changed, as appropriate. *For more information, see Information Access Procedure* An extremely important element of access control. It is referenced in a sub-document (linked) but is important enough to repeat in the main policy.
7 - Approved / Unapproved Equipment and Software	Use / installation of software which has not been approved/issued by the Council is prohibited	Section 7 - No change to wording		
8 - Unauthorised Access or Modification of System	Modification/access to systems without permission is prohibited	Section 8 - No change to wording		
9 - Personal Use	Guidance surrounding personal use of IT	Section 9 - No change to wording	Section 2 - No change to wording	
10 - The Council's Rights and Obligations	Use of Council systems is monitored and any information collected as a result will be processed in accordance with Council's DPA/FOI policies	Section 10 - No change to wording		

APPENDIX 1

Content in 2008 Document	Description of content	Moved in IT Security Policy	Moved in Email/Internet Acceptable Use	Comments from IT
11 - Viruses	Protecting the Council's systems against viruses (including removable media)	Section 11 – Added *For further information, please refer to the Removable Media Protocol.*		
12 - Email Use	Acceptable personal and work related use of the Council's email systems.		Section 3 - see IT comments	12.1 (Email Use) Added: *The sharing of email accounts is not permitted.* Per Email and Internet Access Internal Audit; 02/06/2009; ref. 2.3.3.
12.10 - Telecommunications	Acceptable personal use of the telephone / mobile phones.		Section 3.10 - No change to wording	
13 - Internet Use	Acceptable personal and work related use of the Council's internet		Section 4 - see IT comments	13.1 (Internet Use) Amended: *You may be able to access the internet from the Council's Systems. The internet may be used for legitimate business purposes or for authorised personal use in accordance with section 9. ~~As far as possible,~~ Personal use of the internet should only be used during contractual breaks and outside contractual hours. ~~Excessive~~ Non-job related use of the internet during the working day may be subject to disciplinary action.* Removed ambiguity. 'Excessive' is subject to interpretation.
14 - Use of IT at Home or Out of the Office	Acceptable use of council equipment/systems/ data outside of the	Section 12 – 12.7 added For full details on the use of		

APPENDIX 1

Content in 2008 Document	Description of content	Moved in IT Security Policy	Moved in Email/Internet Acceptable Use	Comments from IT
	office	ICT at home or out of the office, refer to the Mobile and Remote Working Protocol (link not correct)		
15 - Ownership Rights	Work related information remains the property of the Council	Section 13 - No change to wording		
16 - Health and Safety – Display Screen Equipment (DSE) Regulations	Responsibility for H & S.	Section 14 - No change to wording		
		SECTION 15 IS REGARDING BACKUPS		
17 - Harassment and Abuse	Use of technology to harass and abuse others will not be tolerated	Section 16 - No change to wording	Section 5 - No change to wording	
18 - Contraventions of the Policy	High standards expected and system use will be monitored	Section 17 - No change to wording		
19 - Disciplinary Implications	Consequences of misuse	Section 18 - No change to wording	Section 6 - No change to wording	
Acknowledgement and Consent	Acknowledgement of the contents of the policy and	Final section of policy - No change to wording	Final section of policy - No change to wording	

APPENDIX 1

Content in 2008 Document	Description of content	Moved in IT Security Policy	Moved in Email/Internet Acceptable Use	Comments from IT
	confirmation by way of signature that employee agrees to be bound by its terms			

APPENDIX 2

INFORMATION RISK POLICY

1. INTRODUCTION

1.1 Information is a valuable asset that the Council has a duty and responsibility to protect. This responsibility is placed on the Council by the Data Protection Act 1998 monitored and regulated by the Information Commissioner's Office and the Local Public Services Data Handling Guidelines.

1.2 The Information Commissioner's Office now have powers to enable them to impose monetary penalty notices to organisations for up to £500,000 and £50,000 to individuals for breaches of the Data Protection Act, along with having the authority to carry out assessments of organisations to ensure their processes follow good practice.

1.3 The key guidance document that the Council would be measured against is the Local Public Services Data Handling Guidelines Version 2 produced in August 2012 by the Public Services Network in partnership with the Local CIO Council, Socitm, the Cabinet Office and the NLAWARP. The Council therefore has an obligation to comply with these guidelines, to ensure good practice is being followed.

1.4 To ensure that information assets and information systems are used and managed effectively, efficiently and ethically, the Council has produced an Information Charter (see **Appendix 1**), this will work alongside the Information Governance Framework, to ensure everyone is aware of their obligations.

2. PURPOSE OF POLICY STATEMENT

2.1 The purpose and objective of this Information Governance Policy is to protect the Council's information assets from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

2.2 The Council is committed to protecting information through preserving;

Confidentiality: Protecting information from unauthorised access, use and disclosure from unathorised individuals, entities or processes.

Integrity: Safeguarding the accuracy and completeness of information assets. This may include the ability to prove that an action or event has taken place so that it cannot be repudiated later.

Availability: Being accessible and usable on demand by an authorised individual, entity or process.

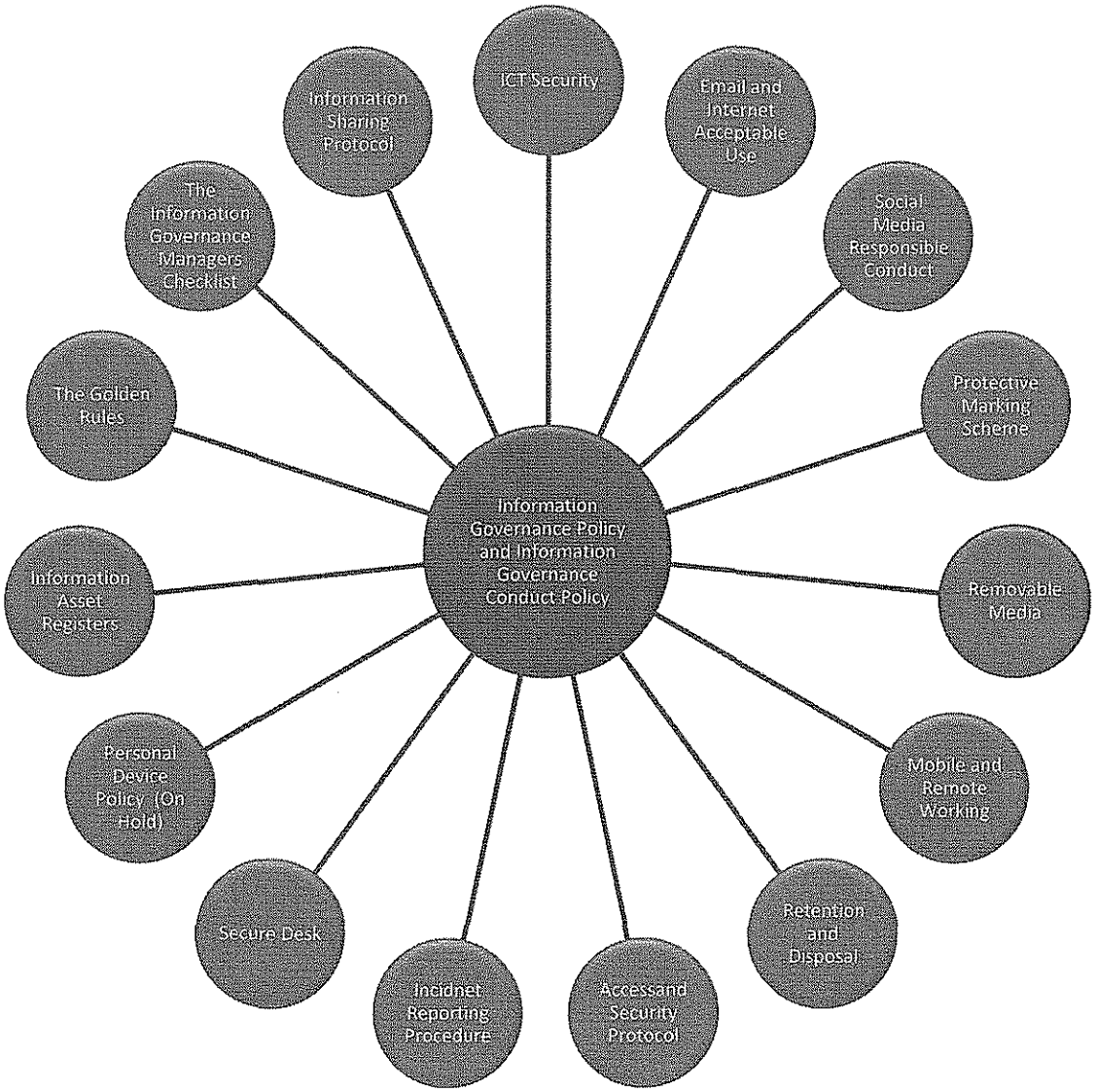
3. INFORMATION GOVERNANCE FRAMEWORK

3.1 This Information Governance Policy is the over-arching document of the Council's Information Governance Framework, (see figure 1 below). The information Governance framework comprises of the Information Governance Policy and Strategy and specific supporting procedures, standards and guidelines as follows:-

- Information Governance Policy and Information Governance Conduct Policy;
- ICT Security;

- Email and Internet Acceptable Use;
- Social Media Responsible Conduct Policy;
- Protective Marking Scheme;
- Removable Media;
- Mobile and Remote Working;
- Retention and Disposal;
- Access and Security Procedure;
- Incident Reporting Procedure;
- Secure Desk Procedure;
- Personal Device Policy (on hold)
- Information Asset Registers
- The Golden Rules
- The Information Governance Managers Checklist
- Information Sharing Protocol;

3.2 Figure 1 – Information Governance Framework



4. SCOPE

4.1 The Information Governance Policy, along with the strategy and all supporting documents, apply to all employees, Members of the Council, temporary staff, contractual third parties, partners or agents of the Council who have access to any information systems or information for council purposes.

4.2 This Information Governance Policy applies to information in all forms including, but not limited to:-

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile telephones, PDA's and laptops;
- Speech, voice recordings and verbal communications, including voicemail; and
- Published web content, for example intranet and internet.

5. INFORMATION GOVERNANCE

5.1 Information Governance is the overall process of analysing, evaluating, assessing and mitigating the impact of risks to an organisation's information and information systems. Information Governance includes physical, personnel and information security and is an essential enabler to making the Council work efficiently. Information risks must be managed effectively, collectively and proportionately, to achieve a secure and confident working environment.

5.2 The Council is aware that risks can never be eliminated fully and it has in place a strategy that provides a structured, systematic and focused approach to managing risk. However risk management is not about being 'risk averse', it is about being 'risk aware'. Some amount of risk taking is inevitable and necessary if the Council is to achieve its objectives. The Council seeks to capitalise on opportunities and to achieve objectives once those decisions are made. By being 'risk aware', the Council is in a better position to avoid threats, take advantage of opportunities and ensure its objectives and goals are realised.

5.3 Information risk will be managed by assigning roles and responsibilities and co-ordinating the implementation of this policy and all supporting documentation. Together these measures form the Information Governance lifecycle and will apply across the Council and in its dealings with all partners and third parties.

6. RESPONSIBILITY FOR INFORMATION GOVERNANCE

6.1 Senior Management (Executive Directors, Assistant Chief Executives, Assistant Executive Directors and Service Unit Managers) has the responsibility and accountability for managing the risks within their own work areas. Employees have a duty to work safely, avoid unnecessary waste of resources and contribute to Governance initiatives in their own

area of activities. The cooperation and commitment of all employees is required to ensure that Council resources are not squandered as a result of uncontrolled risks.

6.2 The Local Public Services Data Handling Guidelines 2008 and the Local Public Services Data Handling Guidelines 2012 introduce some specific roles in relation to Information Governance as follows:-

- Accounting Officer
- Senior Information Risk Owner
- Information Asset Owners

6.3 These specific roles together with the Data Protection Officer and the IT Security Officer will work together with senior management to ensure compliance with best practice with the over-riding objective to keep the Council's information safe.

6.4 Table 1 below details the roles and responsibilities allocated to key staff.

Accounting Officer	The **Accounting Officer** has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. **(Executive Director of Finance/Borough Treasurer)**
SIRO	The **Senior Information Risk Owner** is familiar with and takes ownership of the organisation's information governance policy and strategy. **(Head of Risk Management & Audit Services)**
IAO	**Information Asset Owners** are Directors/AEDs involved in running the relevant Directorate. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets.
SIAO	**Supporting Information Asset Owners** are at Service Unit Level and may have more familiarity with the information assets of that particular area. They are required to feedback to IAO's on what information their service area holds and how it is being managed.
System Owners	**System Owners** are responsible for Information systems. They will ensure system protocols are followed. They have responsibility to recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information systems are accurate and up to date.

Appendix 1

INFORMATION CHARTER

This Charter is for anyone who has dealings with Tameside Metropolitan Borough Council whether through correspondence, involvement in public policy consultations or if for any other reason we hold personal information about you.

The Charter sets out the standards you can expect when we ask for or hold your personal information and what we ask of you, to help us keep information up to date.

We know how important it is to protect your privacy and to comply with the Data Protection Act 1998.

If we ask for your personal information we promise:

- To make sure you know why we need it;
- To ask only for what we need, and not to collect too much or irrelevant information;
- To protect it and make sure nobody has access to it who should not;
- To let you know if we share it with other organisations to give you better public services – and if you can say no;
- To make sure we don't keep it longer than necessary; and
- Not to make your personal information available for commercial use without your permission. Tameside Metropolitan Borough Council does not sell personal information about customers or correspondents to commercial organisations.

In dealing with your personal information, we will also:

- Value the personal information entrusted to us and make sure we respect that trust;
- Abide by the law when it comes to handling personal information;
- Consider the privacy risks when we are planning to use or hold personal information in new ways, such as when introducing new systems;
- Provide training to employees who handle personal information and respond appropriately if personal information is not used or protected properly

In return, we ask you to:

- Give us accurate information; and
- Tell us as soon as possible if there are any changes, such as a new address

This helps us to keep your information reliable and up to date.

APPENDIX 3

INFORMATION GOVERNANCE CONDUCT POLICY

1. INTRODUCTION

1.1 Tameside Metropolitan Borough Council (the Council) has a responsibility under the Data Protection Act 1988 to ensure that the personal information it holds and uses is properly protected. To this effect an Information Governance Framework, which is listed in Appendix 1, has been created to support employees in complying with this responsibility. This conduct policy forms part of the Framework and outlines the expected behaviour of employees regarding information governance. It also indicates the policies and procedures the Council has put in place to keep its personal information safe.

1.2 The Information Governance Conduct Policy applies to all employees, including temporary contract staff and volunteers. It relates to information held both in computerised/electronic systems and paper based records. This includes both work related and personal online activity.

1.3 The Information Governance Conduct Policy sits at the heart of the Information Governance Framework providing information and direction for employees on what is deemed to be acceptable behavior not only when dealing with personal information, but also when generally using systems, electronic communication, the internet or social media. It is not intended to restrict service delivery but to raise awareness of the issues and concerns relating to the variety of information risks faced by the Council.

1.4 The Data Protection Act 1988 is the key piece of legislation covering personal information and the Information Commissioner's Office (ICO) is the regulator and has a range of enforcement actions including the power to fine organisations up to £500,000 for non-compliance.

1.5 The Local Public Services Data Handling Guidelines 2012 outline best practice for protecting information together with resources provided by the Records Management Society, National Archives, Local Authority Information Governance Groups and the ICO.

2. PROCEDURE

2.1 The Council has a number of policies, procedures and guidance documents that form the Information Governance Framework; these will support and provide clarification on information governance.

2.2 Appendix 1 provides a list of each element of the Information Governance Framework with a brief explanation of the content and the key conduct issues from each of the supporting policies, protocols and procedures.

2.3 These policies and procedures which may be amended from time to time, are available on the Council's Intranet (Staff Portal) or on request from the Risk and Insurance Team.

2.4 The table shown in Appendix 2 identifies the mandatory minimum documents for employees to read relevant to their role. It will be the responsibility of Managers to ensure the appropriate documents have been read and to provide clarification for employees of the relevant role if there is any doubt.

3. ROLES AND RESPONSIBILITIES

3.1 Employees are accountable and owe a duty of care to the Council, service users and the residents of Tameside, who they act on behalf of and whose information they handle. It is the responsibility of all employees to ensure their use of the Council's information does not infringe any of the Council's policies and procedures. Or, in turn breach the requirements of the Data Protection Act 1998, the Freedom of Information Act 2004 and the Environmental Information Regulations 2004 or any other applicable legislation.

3.2 Employees have a responsibility of compliance with the Information Governance Framework, when not only handling personal information but also when generally using the internet, any electronic communication or social media. The policies and procedures listed in Appendix 1 will assist with this compliance.

3.3 Managers are responsible for ensuring that employees have appropriate time and support to read the relevant documents and undertake any necessary training. They are also responsible for identifying the relevant policies and procedures for employees to read using the matrix provided. This should be communicated to all employees as part of the induction process, and thereafter as part of team briefings and employee updates. If any assistance is required Managers should contact the Risk and Insurance Manager for advice.

3.4 It is the responsibility of Managers to exercise an appropriate supporting and enforcing role for the identified requirements of the Information Governance Framework to minimise the risk of information loss and breaches of legislation.

3.5 The public is entitled to expect the highest standards of conduct from employees, when handling personal information. Employees role is to serve the Council in providing, implementing its policies and delivering services to the local community. In performing these duties employees must ensure that they understand the requirements placed on them by the Information Governance Framework.

4. CONTRAVENTIONS OF THE POLICY

4.1 Employees need to be aware that this policy and the documents that make up the Information Governance Framework are in place to protect the information held by the Council and to provide assurance to partners, key stakeholders and the Tameside community. Failure to adhere to these framework policies and procedures may lead to disciplinary action being taken and for more serious cases, where individuals have not followed guidance and policies, legal action. In addition it should be noted that an individual fine can be imposed by the Information Commissioner's Office (ICO) in the event that an employee has purposefully used information for an individual's own financial or personal benefit or acted in a highly negligent manner.

APPENDIX 3

Appendix 1

INFORMATION GOVERNANCE FRAMEWORK

Information Governance Policy

The Information Governance Policy and Information Governance Conduct Policy are central to the Information Governance Framework and **must** be read by all employees. Further guidance on the information contained within these documents can be found in the supporting framework documents and an Information Governance Framework Mandatory Documents Matrix can be found at appendix 2 to assist managers and employees in assessing what documents are relevant to their role. To view the Information Governance Policy, click here.

a) ***ICT Security Policy***

This document sets out the responsibilities for using and securing the Council's hardware, software and networks. It details the Council's rights and obligations, and outlines the consequences of using Council Technology in a harassing or abusive manner and the disciplinary implications of not complying with the policy.

Key Conduct Issues

- Protect, at all times, passwords which enable access to data and the Council's network, business systems, email and internet. For further guidance refer to the ICT Service Portal and type 'password' in the search box;
- Never use another person's ICT equipment or device without their permission and with anything other than your own credentials;
- Never use, or install, any software on the Council's systems unless it has been purchased, issued or approved by ICT Services; and
- Always save work related information on the Council's network drives and not on local hard drives. The secure network is backed up and remains available even if your computer fails.
- **For further guidance click here**

b) ***Email, Communications and Internet Acceptable Use Policy***

This policy sets out the expectations of individual's conduct and responsibilities when using the Council's email and Internet facilities, including business and personal use of email (including the personal use of Council and non-Council/personal email accounts). Work related and personal use of the internet (including websites accessed and transactions permitted for work or non-work purposes). It also explains what will happen if Council systems are used for harassment or abuse and the disciplinary implications of not complying with the policy.

Key Conduct Issues

- Never open an email from sources you do not know or trust, and always report unusual emails, suspicious attachments and links, especially in unsolicited emails;
- Never use non-Tameside email accounts to send or receive protected information;
- Use of your @tameside.gov.uk email address is for official Council business, although it can be used for personal business in your own time , this should be kept to a minimum;
- Never send protected information by external email ***unless;***
    - You have a GCSX account and are sending it securely to **another GCSX account** (or other secure government networks) or;
    - You are sending it in an attachment, using a strong password and encryption software.

- Use of the Council's email and internet systems are monitored and activity is logged.
- **For further guidance click here**

c) ***Social Media Responsible Conduct Policy***

This policy applies to all employees whilst participating in any on-line social media activity, whether privately or as part of your role with the Council. It sets out the standards of behaviour the Council expects of all its employees, when using social media services. The disciplinary implications of inappropriate posting on social media websites are explained. It also advises on using social media safely, legally and appropriately and points out that employees are personally liable for what they publish online.

Key Conduct Issues

- Frequent or excessive non-work related use of social media during the working day is not permitted and may result in the withdrawal of some or all access privileges;
- Employees must NOT conduct themselves in a way that is detrimental to the Council and should NOT act in a way which could damage the reputation of the council or the public's trust and confidence in an employee's fitness to undertake their role;
- Never use the Internet in any way to send or post abusive, offensive, hateful derogatory or defamatory messages or comment, especially those which concern members of the public, councillors, employees or the Council; and
- Never post information that could constitute a breach of copyright or data protection legislation.
- **For further guidance click here**

d) ***Protective Marking Scheme***

The Council's Protective Marking Scheme is based on the Government's Protective Marking Scheme. This scheme ensures that information is correctly identified, managed and safeguarded. It lists and explains the types of protective marking and how to assess them. All information which is held, created or modified by Council employees, either electronically or on paper, must be labeled with a protective marking. Failure to protectively mark information could result in a potential breach of the Data Protection Act 1998 and subsequent disciplinary action for the employees involved.

Key Conduct Issues

- Make sure you know what protective marking applies and stick to the rules for that level of protection whenever you have to send protected information, especially outside the Council.
- **For further guidance click here**

e) ***Removable Media Protocol***

This protocol aims to ensure that the use of removable media is securely controlled. All those who have access to or use of removable media are responsible for the safety and security of the media and the information stored on them. Service areas are responsible for implementing this procedure and must monitor the use of removable media. The protocol explains the types of removable media that can be used and the security necessary for use. There is also an explanation of how to dispose of removable media securely. Loss of any unencrypted removable media could result in a potential breach of the Data Protection Act 1998 and subsequent disciplinary action for the employees involved.

Key Conduct Issues

- Only encrypted USB memory sticks purchased through ICT Services may be used in the Council, purchasing must be done through the approved ordering system; Information can only be moved from the Council's systems to an encrypted USB stick
- Information held on removable media should be a short term measure;

- Removable media should be kept secure at all times;
- Removable media should be disposed of securely to minimise the risk of accidental disclosure of sensitive information; and
- All removable media connected to the Council's systems is monitored.

- **For further guidance click here**

f) ***Mobile and Remote Working Protocol***

This protocol applies to any access or use outside Council controlled premises of any ICT Council equipment including mobile telephones, portable devices and static IT equipment. All employees are responsible for the safety and security of portable devices and the information on them, issued to or used by them. Explanations of what physical security is required on the devices and how to use them in line with Council policies and procedures are provided.

Key Conduct Issues

- Always ask yourself *'do you really need to the that information out of the office'* and only take the minimum;
- Do not let unauthorised people, including family members, use of view Council resources and avoid *'shoulder surfers'* in public places viewing your screen or listening to business conversations; and
- Make sure your laptop/device is suitably encrypted and if you have encrypted equipment and protected information in physical files overnight in your home, reduce the risk by ensuring that they are placed out of sight.
- **For further guidance click here**

g) ***Retention and Disposal Schedule***

The schedule outlines the timescales involved for the retention and disposal of information held by the Council. The Retention and Disposal Guidelines will ensure that the information the Council holds is retained for only as long as it is needed to enable it to operate effectively. They also cover the correct disposal methods to be used. Working within the schedule will ensure the Council complies with legislation and the requirements of regulators.

Key Conduct Issues

- Laptops which are no longer required must be returned to ICT enabling the hard drive to be permanently erased;
- Confidential paper waste must be kept separate from ordinary paper waste and protected from accidental loss, damaged or unauthorised access; and
- Information must never be retained for longer than necessary *'just in case'*.
- **For further guidance click here**

h) ***Access and Security Protocol***

This procedure indicates the steps required to ensure that access to Council information, information systems or ICT equipment is controlled. Access needs to be restricted to that needed to perform a role and employees must understand their responsibilities for ensuring the security and confidentiality of information they use. Managers must ensure that access is removed as soon as it is no longer required. It also includes the Leavers and Movers Checklist. As information is held in both paper and electronic format this procedure relates to both physical and technological access.

Key Conduct Issues,

- Only access to systems and information where it is part of your role and you have a legitimate business need to know;
- Where you need protected information 'owned' by another business area to do your job, make sure that authorisation is obtained and that you only ask for the minimum necessary for the required purpose.
- **For further guidance click here**

i) ***Incident Reporting Procedure***

This procedure must be applied as soon as Council information or information systems are suspected to be, or are actually affected by an adverse event which is likely to lead to an Information Security Incident (ISI). All incidents, irrespective of scale, must be reported to ensure that a thorough understanding of what has occurred is recorded, to improve information handling procedures, the incident response process and any subsequent action that may be required.

Key Conduct Issues

- You must always report actual, potential or suspected security violations, problems or vulnerabilities to the Risk and Insurance Manager, ICT Security Officer or Legal Services
- **For further guidance click here**

j) ***Secure Desk Procedure***

This procedure reduces the threat of a security breach as information should be kept out of sight. This procedure applies to all information of a personal, confidential or sensitive nature. It also covers any information that is accessed, viewed or stored within a shared space (i.e. main office, home or Touch Down Point). If non-compliance of this policy results in a breach of the Data Protection Act 1998 subsequent disciplinary action for the employee could arise.

Key Conduct Issues

- Never leave protected information or other valuable assets out on your desk when you are not around;
- Lock your work station when you are away from your desk using *Ctrl + Alt + Delete*, log off at the end of the day and switch off your screen; and
- Remove documents from printers and copiers as they are produced to avoid them being picked up by mistake, or read by someone else.
- **For further guidance click here**

k) ***Personal Device Policy***

This policy states the acceptable ways to access Council systems on employee's personal devices. It outlines that by using a personal device to access the Council's systems and information an individual is accepting responsibility for the safeguarding of information viewed on that device and will be held accountable for any incidents which compromise the safety and security of the Council information they are utilising. Failure to adhere to this policy may lead to disciplinary action being taken and for more serious cases, where individuals have not followed guidance and policies, legal action.

Key Conduct Issues

- You must not download documents containing personal data or other material to your device;
- You must regularly check your device to ensure that no files have been accidentally downloaded and stored on the device (e.g. by accidentally downloading an attachment to an email). Any such file found must be deleted immediately. Unless you are sure that you do not have data on your device you should protect access to your device using a pass code and, where possible, encrypting that device;
- You must not connect your personal device to the Council's private wifi network (although you are permitted to use the free public wifi hotspots located in some Council buildings); and
- Individuals must notify the Council IMMEDIATELY if any of the following occur,
  - a device that has been set up to access the Council's systems is lost,
  - the device has been damaged/has developed a fault,
  - if the device is handed – temporarily or permanently to a third party for repair or other reason.

- **For further guidance click here**

l) ***The Golden Rules***

These Golden Rules aim to help you safeguard the Council's valuable information assets, systems and equipment. They briefly outline how to use information assets responsibly within the framework of the law and ensure employees understand the corporate policies to comply with. It signposts the mandatory corporate on-line training employees must undertake. All employees must comply with the minimum corporate security standards set out in these rules which are based on the Council's Information Governance Framework. Employees also need to adhere to any localised business specific data handling requirements. **Click here for the Golden Rules**

m) ***Information Governance Managers Checklist***

This checklist has been provided for Managers/Supervisors to enable them to identify the areas they should be considering on a regular basis to ensure compliance with the Information Governance Framework. It also details the available resources to assist Managers/Supervisors in complying with the appropriate actions required. **Click here for the Information Governance Managers Checklist**

n) ***Information Sharing Protocol***

This protocol is the overarching document that outlines the responsibilities of employees when sharing information. It applies to all sharing of information, potentially internally and externally to the Council. Information Sharing or Processing Agreements will govern specific exchanges of information and will specify what information is to be shared, how it will be shared and for what purpose the information is required. Failure to comply with this protocol, when sharing information would constitute a breach of the Data Protection Act 1998 and could result in disciplinary action.

Key Conduct Issues

- Before disclosing protected information to an external third party, always ask yourself '*is this request legitimate'* and ' *do I need a sharing or processing agreement';*
- Always make sure you have the legal authority to share;
- Check whether the purpose could be satisfied with anonymised or pseudonymised information; and
- Keep a documented audit trial of all disclosures.
- ***For further guidance please click here***

APPENDIX 3

Appendix 2

Information Governance Framework Mandatory Documents Matrix

Framework Document	Managers	Office Based Employees	Office Based with some Home Working	Mobile Working	Care Workers	Manual & Outdoor Workers
Information Governance Policy	✓	✓	✓	✓	✓	✓
Information Governance Conduct Policy	✓	✓	✓	✓	✓	✓
ICT Security	✓	✓	✓	✓	✓	✓
Email/Internet Acceptable Use	✓	✓	✓	✓	✓	✓
Social Media Policy	✓	✓	✓	✓	✓	✓
Protective Marking Scheme	✓	✓	✓	✓	✓	-
Removable Media	✓	✓	✓	✓	✓	-
Mobile/Remote Working	✓	✓	✓	✓	✓	-
Retention and Disposal	✓	✓	✓	✓	✓	-
Information Access Procedure	✓	-	-	-	-	-
Information Reporting Procedure	✓	✓	✓	✓	✓	✓
Secure Desk	✓	✓	✓	✓	✓	-
Bring your own Device	✓	✓	✓	✓	-	-
Information Sharing Protocol	✓	**If Applicable**	**If Applicable**	**If Applicable**	**If Applicable**	-
Golden Rules	✓	✓	✓	✓	✓	-
Managers Checklist	✓	-	-	-	-	-

APPENDIX 4

ICT SECURITY POLICY

1. INTRODUCTION

1.1 IT is an increasingly integral part of the Council's activities and is essential in the delivery of most services. Almost all Council employees and Councillors will use Council ICT in the course of their duties. This policy is designed to enable the Council to:

- get the best return possible for the investment it has made in technology
- Comply with the law
- minimise legal and other risks associated with the use of technology
- ensure effective running of the Council's business
- minimise the risk of disruption caused by computer viruses and inappropriate us of IT; and
- provide clear information to employees and councillors and increase ICT skills of our employees and resident

1.2 This policy sets out the Council's policy on using its computers and networks, including all devices such as telephones, mobile phones; faxes; printers, scanners and anything of an electronic nature otherwise referred to as information technology etc. This equipment is for clarity of understanding referred to throughout this policy as the Systems.

1.3 This policy applies to all Council employees and Members who use the Systems. It also applies to other people using the Systems such as agency workers and contractors' staff.

1.4 Where this policy says that something is not permitted without the Council's permission it means that you need the written permission of your Service Unit Manager or above or the Head of ICT Services.

1.5 The Council's Systems are the property of Tameside MBC. In order to protect the Systems, the Council reserves the right to amend any of the policies and procedures set out in this document from time to time, following due consultation with the relevant trades unions.

2. USER RESPONSIBILITY

2.1 All users have responsibility for the technology they use. Responsibility extends from the Service Unit Manager who oversees a complete system to individual employees with a PC on their desk. Everyone using IT must observe the following:

- ***Equipment Purchase/Disposal*** – all Council equipment must be purchased through ICT Services using the e-procurement facility. All equipment must be disposed through ICT services to ensure that legislation is complied with both in respect of the environment and security of information. Changing hard drives; moving ICT equipment or disposing of it without taking appropriate measures to keep information secure is likely to result in confidential information becoming available to persons not entitled to the data and consequentially breaches in statute –requirements to be followed can be found at http://intranet2.tameside.gov.uk/security/equipment.htm
- ***Equipment Maintenance*** - if equipment malfunctions you should contact the IT helpdesk for advice and assistance. Employees are not permitted to attempt to repair or maintain their IT equipment, except for day-to-day needs such as replacement ink cartridges in printers etc. Equipment must be kept clean, especially screens and keyboards, and this is a responsibility of the employees using the equipment.
- ***Accidental Damage*** - employees are expected to make efforts to avoid circumstances that may result in accidental damage, such as spilt coffee or equipment being dislodged off desks

- ***Keep Equipment Secure*** - employees should ensure that the equipment provided is kept secure from theft. This particularly applies to portable equipment such as laptop computers and mobile phones. Equipment is not necessarily insured if it is outside Council premises (for example if it is left in a car). If Equipment is lost or damaged as a result of an employee's negligence then disciplinary action may be taken and the Council may take action to recover the loss from the employee concerned. Any queries about this should be referred to Internal Audit/Insurance.
- ***Equipment Insurance*** – ICT equipment is not insured if it is outside Council premises, (e.g. if it is left in a car) unless it is a laptop/tablet computer. However these portable items are only covered within the UK and must be secured when not in use. Any queries about this should be referred to Risk and Insurance.

3. MANAGEMENT OF DATA, INFORMATION AND SOFTWARE

3.1 Employees are expected to manage data in compliance with the law, particularly the law relating to data protection and freedom of information. Separate guidance about this is available on the intranet, but the main principles are that employees must:

- ***Keep data accurate and up to date and retain for no longer than necessary;***
- ***Keep Data Secure; and***
- ***Keep Data Confidential*** – The Council has legal duties under the Data Protection Act 1998 and the Computer Misuse Act to protect the information that it holds. No personal information should be disclosed unless you are sure that you are permitted to do so. When sharing such information with third parties, checks should be made to ensure that third parties are registered as a data controller under the Data Protection Act 1998. Your manager or supervisor will be able to advise you in the first instance. If any employees have any further queries they should seek advice from the Council's statutory Monitoring Officer who is also the Data Protection Officer – Borough Solicitor.

4. AUTHORISED BUSINESS USE

4.1 You may use the Systems where you have a legitimate business need to do so and the use is appropriate to your role or you are using the Systems for appropriate personal use in accordance with section 9 of this policy.

4.2 In order to ensure accountability in the use of the Systems, you must never use any computing device without the permission of the main allocated user.

4.3 Communications sent via the Systems represent the Council. Therefore, you must ensure that all messages, communications and information created by you on the Systems are professional in tone and content. The style and language of any messages, communications or information you create should be in accordance with standard business communications and any corporate formatting and style requirements.

5. UNAUTHORISED USE

5.1 You must never use the Council's Systems to:

- Create, review or transmit material that is offensive, untrue, defamatory, malicious, potentially damaging to the Council's reputation or disruptive in nature. In particular you are not permitted to use the Systems to create, review or transmit material containing inappropriate sexual references, discriminatory, harassing or threatening comments, or any other form of communication that would be deemed offensive in nature and contrary to the Council's employment policies, specifically the Council's Equal Opportunities Policy, Bullying and Harassment Policy and Data Protection

Policy. For the avoidance of doubt this includes but is not limited to material containing nudity, racist remarks, and/or defamatory material

- Access any part of the IT facility beyond the facilities available from the main user menus or icons unless you have the Council's permission to do so;
- Use any software that has not been officially purchased, issued or approved
- Copy any of the software on the Council's computer Systems without the authorisation of the Council. Software will be audited on a regular basis
- Alter the configuration of the Council's Systems, hardware or software, without prior authorisation by the Council's ICT Service (Please note: Use of approved end user software applications such as Microsoft Excel does not constitute alteration of configuration of Council Systems
- Create or circulate chain letters or jokes; nor
- Play computer games

6. PASSWORDS AND SECURITY

6.1 You will be issued with passwords for accessing the Council's Systems. You must keep your password confidential and you should not disclose your password to anyone else unless you have been authorized to do so by the Council. You must not write down your passwords or display them where they could be seen by others. You must take care to see that people do not see you entering your password.

6.2 It is the Council's policy that passwords should, be changed at regular intervals. During the course of your employment you are likely to be responsible for creating some of your own passwords. When creating a password, you should not select a password that can easily be deduced by others; in particular, you should not use passwords which are easy to guess (e.g. the names of partner children or pets). It is advisable to use a mix of characters, e.g. 3 out of four of: upper or lower case alphabetic characters, numbers and symbols in each password. For further guidance please refer to the ICT Service Portal for Password Guidance. Click here and type 'password' in the search box

6.3 When you have logged into any computer you should ensure that it is left securely so that no unauthorised person can access them. On PCs you can do this by selecting control, alt, delete and using the menu to lock your computer

6.4 Personal or confidential data belonging to or held by or on behalf of the Council or its partners must not be stored on removable media, such as USB memory sticks CDs or external hard drives without the express permission of the Council. Where such information is unavoidably stored on a memory stick, it must be encrypted so that if it is lost or stolen the data cannot be viewed and/or misused. For further information, please refer to the Removable Media Protocol.

6.5 When an employee leaves the Council, their access to computer systems and data must be deleted on the employee's last working day. It is the responsibility of the line manager to request access deletion via the ICT Service Desk. Similarly, HR must inform ICT Services when any employees change jobs within the Council so that systems can be amended and the user's systems access changed, as appropriate. For more information, see the Information Access Procedure

7. APPROVED / UNAPPROVED EQUIPMENT AND SOFTWARE

7.1 You must not use or install any software on the Systems unless that software has been approved and issued by the Council. For example you must not install or run software that you have brought in from home, downloaded from the internet or other IT Systems. This is to avoid conflicts between software, damage to Systems or breaking copyright law. The

ban on installing or downloading software unless specifically authorised by the Council includes a ban on installing or downloading:

- Games
- Freeware and shareware
- Upgrades to existing software
- Demonstration versions of software
- Screensavers

7.2 You must not connect any equipment to the Council's Systems unless it belongs to the Council or you have the Council's permission.

8. UNAUTHORISED ACCESS OR MODIFICATION OF SYSTEMS

8.1 Unless you have been authorised by the Council to do so you must not, nor attempt to, modify the Council's Systems. (Please note: Use of approved end user software applications such as Microsoft Excel does not constitute modification of Council Systems.)

8.2 You must not misuse the Council's Systems by accessing information which you are not authorised to view or use, or to attempt to break ('hack') into any computer system, for example by using someone else's password

9. PERSONAL USE

9.1 The Council has devoted time and effort into developing the ICT Systems to assist you with your work. The Council does, however, recognise that there are times when you may want to use the Systems for non-work related purposes, and in recognising this need the Council permits you to use the Systems for personal use.

9.2 You must not use the Systems for personal use during working hours. If you work flexible hours then personal use must be at a time when you are not working and outside core time. You must not allow personal use of Systems to interfere with your day to day duties Excessive non-job related use of the Systems during contractual hours may be subject to disciplinary action

9.3 You must not use Council software for personal use unless the terms of the licence permit this and you are responsible for checking the licensing position. Microsoft Office and Internet Explorer are licensed for personal use.

9.4 Use of the Systems should at all times be strictly in accordance with the provisions of paragraph 5.1 above. You must pay all costs associated with personal use at the Council's current rates e.g. cost of paper and telephone calls

9.5 You are responsible for any non business related file which is stored on your computer. If you connect your personal memory stick to any system you must carry out appropriate virus checks first.

9.6 When accessing the internet for non work purposes you may only view web pages and download .pdf files. You may not download other files because they contain a risk of contamination by viruses and that risk is disproportionate to the benefits to the Council in allowing you access to them

10. THE COUNCIL'S RIGHTS AND OBLIGATIONS

10.1 The Council reserves the right to monitor all communications and information created, or transmitted on the Systems in order to protect the Council's legitimate business interests and the Systems. These include, but are not limited to, ensuring compliance with policies, detecting or preventing crime, recording evidence of business transactions and detecting viruses. You should not therefore expect communications conducted on the Council's Systems to be private

10.2 Any information that the Council collects as a result of monitoring the use of its Systems will be processed in accordance with the Council's Data Protection and Freedom of Information Policies

11. VIRUSES

11.1 Computer viruses have the potential to cause enormous damage to Systems and the data they hold, and severely affect service delivery as a result. Every effort must be made to avoid introducing viruses into the Council's Systems and equipment, and employees have a clear responsibility in this respect. Employees must ensure that ANY disk or memory stick being brought into the Council is virus checked before loading. If a PC does not have its own virus checking software then the IT Helpdesk should be contacted

11.2 Viruses may be transmitted through E-mails and/or attachments. If anyone has any doubt about an e-mail received, especially from an unknown source, refer it to the IT Helpdesk. Do not open any suspicious e-mail or attachment. Any employee who intentionally or negligently causes a virus to affect Council Systems is liable to disciplinary action. It is essential that all employees remain vigilant

11.3 To prevent viruses damaging the Systems all computer Systems must have the appropriate anti-virus software installed and this must be updated regularly. The anti-virus software should never be disabled. All files used on Council computer Systems will be scanned automatically but for added security you should take due precautions when using any external device or media such as CDs, USB memory sticks and the like and satisfy yourself that they are virus free. For further information, please refer to the Removable Media Protocol.

12. USE OF IT AT HOME OR OUT OF THE OFFICE

12.1 The provisions of the Policy apply equally when working on Council data or equipment outside Council premises

12.2 If employees are working from home on a regular/permanent basis then specific arrangements must be agreed with your Service Unit Manager.

12.3 Employees must not install Council owned software on their own equipment or connect Council owned equipment to their personal equipment

12.4 The Council cannot be held liable if, for any reason, the use of personally owned equipment for Council business results in that equipment being damaged or adversely affected in any way

12.5 Data must be kept securely. Employees must not use their own equipment to process personal data without the agreement of their Service Unit Manager, who must ensure that proper arrangements for the security of the data are made

12.6 You must not store Council files on your personal equipment. You should use a Council memory stick, which is encrypted, to store such files when working on them at home. Care should be taken to ensure that

a) You do not store files on your computer; and
b) When you dispose of any IT equipment you make sure that no Council documents have accidentally been stored on it and none are stored in any temporary folder – or you remove and destroy the computer's hard drive

12.7 For full details on the use of ICT at home or out of the office, refer to the Mobile and Remote Working Protocol

13. OWNERSHIP RIGHTS

13.1 Work related information, communications or data created, received, stored or transmitted by you whilst you are employed by the Council (whether inside or outside of working hours) is and remains the property of the Council

14. HEALTH AND SAFETY – DISPLAY SCREEN EQUIPMENT (DSE) REGULATIONS

14.1 All employees have responsibility for Health & Safety in the workplace, and this will be reflected in the manner that IT is used. Employees and Service Unit Managers are expected to ensure that the use of technology in their areas complies with the provisions of Health and Safety legislation. Employees and Service Unit Managers are expected to ensure that the workplace is kept tidy, and that the presence of technology in the office is not a cause for concern.

14.2 So far as the Council is concerned, an employee falls within the requirements of the Display Screen Equipment (DSE) regulations if they use equipment for continuous spells of an hour or more (on average) every day. The requirements of the DES regulations can be found here and all employees and Managers should comply with it

15. BACK UPS

15.1 It is vital that backup procedures are in place to maintain the availability, integrity and confidentiality of data. ICT Services backup the corporate servers on a regular basis.

15.2 All employees must be aware that ICT only back up information stored on the network (shared drives). Information stored on local (C:) drives is not backed up and would not be able to be recovered if the equipment was lost, corrupted etc. Therefore, information stored on local drives should be kept to a minimum.

15.3 Service Unit's are responsible for ensuring that appropriate backups are undertaken for any local drives or standalone PCs located in their service area.

16. HARASSMENT AND ABUSE

16.1 The use of technology to harass and abuse others will not be tolerated. The Council has a clear and fundamental commitment to equal opportunities and the welfare of its employees, Councillors and others; and will not tolerate harassment in any form. This commitment is made explicit in the current 'Bullying and Harassment' policy. Any employee found to be using technology as a means of harassing others will be investigated and disciplinary action

will be taken as appropriate. This applies whether it is another employee, a councillor, or a member of the public who is subject to the harassment or abuse

16.2 Employees should be aware that the Council Systems including the internal and external e-mail system may be monitored from time to time to ensure that the system is not being abused, to ensure that this code of practice is being complied with and for any other lawful purpose

17. CONTRAVENTIONS OF POLICY

17.1 Local Government employees are expected to give the highest possible standard of service to the public. Employees are expected, through agreed procedures and without fear of recrimination, to bring to the attention of the Council any deficiency in the provision of service. Employees should report to the appropriate manager any impropriety or breach of procedure or misuse of Council property. The Council has a Whistle Blowing Policy in place to encourage and protect responsible employees to come forward, anonymously if they wish, to report instances of abuse of time, etc.

17.2 Employees should be aware that the Council Systems including the internal and external e-mail system may be monitored from time to time to ensure that the system is not being abused, to ensure that this code of practice is being complied with and for any other lawful purpose

18. DISCIPLINARY IMPLICATIONS

18.1 Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the *Computer Misuse Act 1990*, and may lead to prosecution of the Council and the individual(s) concerned and/or civil claims for damages

18.2 Most use of IT is by employees and the code has been written with them in mind. However, it applies equally to Councillors using Council owned IT. Mis-use of Council owned IT equipment or software may be a breach of the statutory Code of Conduct for Councillors - in which case it may be reported to the Standards Board for England and/or the Council's Standards Committee who may impose a sanction

APPENDIX 5

EMAIL/COMMUNICATIONS/INTERNET ACCEPTABLE USE POLICY

1. INTRODUCTION

1.1 IT is an increasingly integral part of the Council's activities and is essential in the delivery of most services. Almost all Council employees and Councillors will use Council ICT in the course of their duties. This policy is designed to enable the Council to:

- get the best return possible for the investment it has made in technology
- gain maximum benefit from email and the internet
- comply with the law
- minimise legal and other risks associated with the use of technology
- ensure effective running of the Council's business
- minimise the risk of disruption caused by computer viruses and inappropriate us of IT; and
- provide clear information to employees and councillors and increase ICT skills of our employees and resident

1.2 This policy sets out the expectations of individual's conduct and responsibilities when using the Council's email and Internet facilities, including;

- Business and personal use of email (including the personal use of Council and non-Council/personal email accounts)
- Work related and personal use of the internet (including websites accessed and transactions permitted for work or non-work purposes)
- Business and personal use of social media (including the posting of information on social media sites whether related or unrelated to any Council business)

1.3 This policy applies to all Council employees and Members who use the Systems. It also applies to other people using the Systems such as agency workers and contractors' staff.

1.4 Where this policy says that something is not permitted without the Council's permission it means that you need the written permission of your Service Unit Manager or above or the Head of ICT Services.

1.5 The Council's Systems are the property of Tameside MBC. In order to protect the Systems, the Council reserves the right to amend any of the policies and procedures set out in this document from time to time, following due consultation with the relevant trades unions.

2. PERSONAL USE

2.1 The Council has devoted time and effort into developing the ICT Systems to assist you with your work. The Council does, however, recognise that there are times when you may want to use the Systems for non-work related purposes, and in recognising this need the Council permits you to use the Systems for personal use.

2.2 You must not use the Systems for personal use during working hours. If you work flexible hours then personal use must be at a time when you are not working and outside core time. You must not allow personal use of Systems to interfere with your day to day duties Excessive non-job related use of the Systems during contractual hours may be subject to disciplinary action.

2.3 You must not use Council software for personal use unless the terms of the licence permit this and you are responsible for checking the licensing position. Microsoft Office and Internet Explorer are licensed for personal use.

2.4 Use of the Systems should at all times be strictly in accordance with the provisions of paragraph 5.1 above. You must pay all costs associated with personal use at the Council's current rates e.g. cost of paper and telephone calls.

2.5 You are responsible for any non business related file which is stored on your computer. If you connect your personal memory stick to any system you must carry out appropriate virus checks first.

2.6 When accessing the internet for non work purposes you may only view web pages and download .pdf files. You may not download other files because they contain a risk of contamination by viruses and that risk is disproportionate to the benefits to the Council in allowing you access to them.

3. EMAIL USE

3.1 The Council has developed its email system to facilitate effective business communication within the workplace. You are only permitted to use the email system for personal use in accordance with section 9 above – though you should be aware that all emails may be subject to monitoring and the right to send personal emails implies no confidentiality. All emails that you create should adhere to the provisions of this policy, and in particular comply with the requirements set out in section 3.

3.2 Employees should treat e-mail communications with the same degree of care and professionalism as they would a letter sent out on company-headed notepaper. They should all meet ' the Chief Executive Test' namely would the Chief Executive send this email out on behalf of the Council or more importantly would this e-mail give the Chief Executive cause for concern if she saw it? E-mail is not a suitable medium for the communication of confidential, personal, or other sensitive information, nor for communication on any other matter, which requires dialogue or discussion and should not be used as a substitute for face-to-face communication. The sending, or forwarding on, of curt, rude, sexually explicit, racially biased or offensive e-mails (or attachments) is strictly prohibited. Equally, employees are advised not to send e-mails in the heat of the moment. Employees should not send unsolicited, irrelevant, or inappropriate e-mail messages internally or externally, nor should they participate in chain or pyramid letter by e-mail. Furthermore, personal opinions should not be presented as if they were those of the Council. E-mails should be courteous and written in a style appropriate to business communication and not in a casual or flippant tone. Careless or casual use of humour should be avoided, as it can be misinterpreted. The sending, or forwarding on, of jokes by e-mail (or as an attachment) is strictly prohibited.

3.3 You should not use the email system in breach of any of the Council's employment policies, particularly the Council's Equal Opportunities Policy, Bullying and Harassment Policy and Data Protection Policy. Employees must not use the e-mail system to send inappropriate messages or images via the email system (whether internally or externally). Inappropriate messages would include those, which are:

- Sexually explicit
- Offensive (whether to the recipient or to a third)
- Potentially damaging to the Council's reputation and/or standards expected by the public
- Defamatory
- Discriminatory (e.g. racist or sexist)
- Constitute harassment (see section 7)

3.4 E-mail is a `publication` for the purposes of the law. Any e-mail that includes information taken from another source [such as a publication or a website] may also breach copyright,

for which the Council may be held responsible. Messages sent via the email system can give rise to legal action against the Council. Claims of defamation, harassment and breach of confidentiality or contract could arise from a misuse of the Systems. Email messages are disclosable in any legal action commenced against the Council relevant to the issues set out in the email. Employees should note that E-mail messages and any attachments can be used as evidence in many circumstances and may have to be disclosed under the Freedom of Information Act. You must use the Council's email disclaimer on emails along with a signature file providing contact details. Anyone found to be sending or forwarding inappropriate messages, or exposing the authority to legal action, may be subject to disciplinary action.

3.5 As with other forms of business communications, you should retain copies of the emails you send, where necessary, for an appropriate length of time.

3.6 Unless you have been granted permission to do so by the Council, you should not send confidential information by email. Confidential information means all information which may be imparted in confidence or be of a confidential nature including but not limited to all information relating to the Council's business or prospective business. It is important to remember that email sent over the internet is not secure. You should not therefore send any confidential information by external email unless it is properly encrypted or you have the Council's permission to do so. Email sent by Government Connect (where available) is considered to be secure.

3.7 If an email message is sent to you in error, you should contact the sender. If the email message contains confidential information you must not disclose or use that confidential information. If you receive an email of this nature you should contact your immediate line manager.

3.8 You should only open emails with attachments from persons or organizations that you are familiar with. If you receive an email with an attachment from an unknown source and you are suspicious as to the nature of the communication you should forward the email to ICT Services to inspect before opening it. You should not open any emails which do not appear to relate to Council business and seem to contain jokes, graphics or images; as such emails regularly contain viruses.

3.9 Employees are permitted to send and receive personal email whilst at work (in accordance with section 9 above) but emails must not contain inappropriate content. Employees must not send or receive excessive numbers of personal emails and must not allow their Council email account to be used for commercial (non-Council) purposes. Excessive or inappropriate use of email may lead to disciplinary action and to withdrawal of some or all privilege.

4. TELECOMMUNICATIONS

4.1 Employees are allowed to use the Council telephone system [and mobile telephones provided by the Council] for personal calls. However, where a cost is incurred employees will reimburse the Council with the cost of the call. Employees will not use telecommunications Systems and equipment provided by the Council for any activity that is illegal, for harassment or abuse of others, or for personal gain. Any employee found doing so may be liable for disciplinary action.

4.2 Interception and Monitoring: This Policy has been prepared in accordance with the Data Protection Act, the Human Rights Act, and the Regulation of Investigatory Powers Act 2000. Exceptionally, the Council may monitor and/or intercept telecommunications Systems where permitted by the Regulation of Investigatory Powers Act 2000.

5. INTERNET USE

5.1 You may be able to access the internet from the Council's Systems. The internet may be used for legitimate business purposes or for authorised personal use in accordance with section 9. As far as possible, personal use of the internet should only be used during contractual breaks and outside contractual hours. Excessive non-job related use of the internet during the working day may be subject to disciplinary action. Internet access may be withdrawn if it is being abused. Employees should be aware that all visits to websites on the Internet are logged and monitored by software operating on the Councils web server and may be subject to audit and inspection.

5.2 You should note that there are a number of inherent risks involved in using the internet, particularly a lack of confidentiality when transmitting information. Viruses can be spread by software or other files being downloaded from the internet, and you should not download information or files from the internet unless you have a business need to do so and are satisfied that the information you intend to download does not present any security risks. Advice from IT Services is available about this. You should also try to ensure that you will not be infringing any copyright or related rights, by downloading the information.

5.3 You must not access, view or download any illegal or inappropriate material. In particular, you should not access, view or download any material that would constitute a breach of the Council's Equal Opportunities Policy and/or the Council's Bullying and Harassment Policy.

5.4 You should note that, in order to protect its legitimate business interests and its Systems, the Council monitors internet use in accordance with the provisions set down in section 10, above.

5.5 The Council has installed software to try to prevent access to inappropriate web pages. This includes pornography and illegal sites as well as gambling and racist sites. The risk of viruses and other malware also means that access to web-based email services is considered inappropriate. However the system relies on a list of banned sites and key word searches and so is not completely comprehensive. Employees are not permitted to access any site with inappropriate content and may be subject to disciplinary action if they do. Exceptionally, employees may need to access this type of site for work related purposes. If this need arises they must seek written authority to do so from the Head of ICT; the Internal Audit Manager or the Council's Monitoring Officer in advance.

5.6 It may, very rarely, happen that despite the protection Systems, an employee accidentally visits an inappropriate site. If this happens then they must inform the Head of ICT and the Internal Audit Manager immediately by e-mail to avoid the possibility of being suspected of seeking to access inappropriate web pages.

5.7 Employees may use the internet to carry out their own private transactions (e.g. the purchase of books or tickets) but you may not carry out transactions, which would be viewed as inappropriate under other parts of this Policy. IT Systems are not entirely secure. The Council will not accept any responsibility for any loss that you may suffer as a result of personal use of the internet. Employees are reminded that the Council may monitor internet use.

6. HARASSMENT AND ABUSE

6.1 The use of technology to harass and abuse others will not be tolerated. The Council has a clear and fundamental commitment to equal opportunities and the welfare of its employees, Councillors and others; and will not tolerate harassment in any form. This commitment is made explicit in the current 'Bullying and Harassment' policy. Any employee found to be using technology as a means of harassing others will be investigated and disciplinary action

will be taken as appropriate. This applies whether it is another employee, a councillor, or a member of the public who is subject to the harassment or abuse.

6.2 Employees should be aware that the Council Systems including the internal and external e-mail system may be monitored from time to time to ensure that the system is not being abused, to ensure that this code of practice is being complied with and for any other lawful purpose.

7. DISCIPLINARY IMPLICATIONS

7.1 Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted under the *Computer Misuse Act 1990*, and may lead to prosecution of the Council and the individual(s) concerned and/or civil claims for damages.

7.2 Most use of IT is by employees and the code has been written with them in mind. However, it applies equally to Councillors using Council owned IT. Mis-use of Council owned IT equipment or software may be a breach of the statutory Code of Conduct for Councillors - in which case it may be reported to the Standards Board for England and/or the Council's Standards Committee who may impose a sanction.

APPENDIX 6

SOCIAL MEDIA USE: RESPONSIBLE CONDUCT POLICY FOR TAMESIDE COUNCIL STAFF AND MANAGERS

As an organisation, we encourage communication among our employees, residents, customers, partners, and others - and Web logs (blogs), social networks, discussion forums, wikis, video, and other social media - such as Twitter - can be a great way to stimulate conversation and discussion. They are also an invaluable tool to share information and consult:

The Internet provides a number of benefits in which Tameside council employees may wish to participate. From rediscovering old school friends on *Facebook* to keeping up with other people's daily lives on *Twitter* or helping to maintain open access online encyclopaedias such as *Wikipedia*. Even if your social media activities take place completely outside of work, as your personal activities should, what you say can have an influence on your ability to conduct your job responsibilities, your work colleagues' abilities to do their jobs, and Tameside's business interests.

Accordingly, where an employee is clearly identifiable as being an employee of the Council and/or discusses their work, they are expected to behave appropriately when on the Internet, and in ways that are consistent with the Council's values and policies. This guidance note sets out the principles which Council employees are expected to follow when using the Internet and gives interpretations for current forms of interactivity. It applies to blogs, to microblogs like *Twitter* and to other personal webspace. The Internet is a fast moving technology and it is impossible to cover all circumstances. However, the principles set out in this document should always be followed.

The intention of this guidance is not to stop Council employees from conducting legitimate activities on the Internet, but serves to flag-up those areas in which conflicts can arise.

Tameside Council's reputation for impartiality, objectivity and fairness is crucial. The public must be able to trust the integrity of Tameside councillors, employees and it services. Our residents and partners audiences need to be confident that the outside/private activities of our employees do not undermine the Council's reputation and that its actions are not perceived to be influenced by any commercial or personal interests.

To this end employees:

- Should NOT engage in activities on the Internet which might brings the Council into disrepute
- Should NOT conduct themselves in a way that is detrimental to the Council.
- Should NOT use the Internet in any way to send or post abusive, offensive, hateful or defamatory messages, especially those which concern members of the public, councillors, employees or the Council.
- Should NOT post derogatory or offensive comments on the Internet
- Should NOT act in a way which could reputationally damage the council.
- Should NOT act in a way that damages the Council's or the public's trust and confidence in an employee's fitness to undertake their role.
- Should act in a transparent manner when altering online sources of information.
- post information that could constitute a breach of copyright or data protection legislation;
- employees should only use their @tameside.gov.uk email addresses for official Council business.
- use the Council's ICT Systems for party political purposes or for the promotion of personal financial interests; and
- take care not to allow interaction on these websites that could cause damage to working relationships between councillors, employees and the public

Even if they are not identified as a Tameside employee, staff in politically restricted posts (usually over salary scale point 44) and in politically sensitive areas should not be seen to support any political party or cause. Any online activities associated with work for the Council should be discussed and approved in advance by a line manager.

All staff should be mindful of the information they disclose on social networking sites. Where they associate themselves with the Council (through providing work details or joining a council employee network) they should act in a manner which does not bring the Council into disrepute.

Employees will be aware that use of the internet at work is provided primarily for business use. However the Council recognises that many employees use the internet for personal purposes and that many employees participate in social networking on websites such as Facebook, Twitter, MySpace, Bebo and Friendster (this list being for illustrative purposes only). Alongside such social networking sites the internet also offers employees the opportunity to access and post on blogs, twitter, wikis and other online forums.

The purpose of this guidance is to outline the responsibilities of employees using social networking websites and other online forums. It forms part of the Council's existing ICT and E-mail Security Policy and the Councils employee Code of Conduct.

Personal use of the internet at work
The Council has devoted time and effort into developing the ICT Systems to assist you with your work. The Council does, however, recognise that there are times when you may want to use the ICT Systems for non-work related purposes, and in recognising this need the Council permits you to use the ICT Systems for responsible personal use.

You must not use the ICT Systems for personal use during working hours. If you work flexible hours then personal use must be at a time when you are not working and outside core time. You must not allow personal use of the ICT Systems to interfere with your day-to-day duties or of others.

If you choose to use the Council's ICT Systems to access social networking sites and/or other online forums, blogs etc you must do so in a responsible and appropriate manner. There is no unconditional right for an Employee to access such sites and the Council reserves the right to restrict access to the internet (or certain websites) for particular employees if there is cause for concern over their use.

Employees should be aware that social networking websites are a public forum, particularly if the employee is part of a "network". Employees should not assume that their entries on any website will remain private.

Personal conduct whilst in work or outside the workplace
The Council respects an employee's right to a private life. However, the Council must also ensure that confidentiality and its reputation are protected.

Employees are reminded of the unique way in which information posted on the internet can be quickly disseminated and control over such information can be rapidly lost. As such, employees should think about what information they are posting and how this could reflect on them and the Council especially in light of the difficulty they may encounter in trying to remove such information.

Employees using social networking websites and/or online forums outside of work are requested to:

- Refrain from identifying themselves as working for the Council. However, If you comment on any aspect of the Council's business or any Council policy issue, you must

clearly identify yourself as a Tameside employee in your postings or blog site(s) and include a disclaimer that the views are your own and not those of the Council.

- Ensure that they do not conduct themselves in a way that is detrimental to the Council;
- Never send or post abusive, offensive, hateful or defamatory messages about members of the public, councillors, other employees or the Council
- Take care not to allow interaction on these websites that could cause damage to working relationships between councillors, employees and/or members of the public.

Monitoring of online access at work

You should note that, in order to protect its legitimate business interests and its ICT Systems, the Council monitors internet use in accordance with the provisions set down in the ICT and Email Security policy.

Inappropriate Posting

If an employee is found to have posted inappropriate material in any format on the internet, they are required to assist in any way to ensure such material is removed without delay. Failure to assist in removing such material in a timely fashion could lead to disciplinary action being taken against that employee.

Disciplinary Implications

If the Council finds that an employees' internet use is not in accordance with the ICT policy or this guidance, access to the internet may be withdrawn.

Employees are reminded they should never send or post inappropriate, abusive or defamatory messages on the internet either whilst in work or outside the workplace. Any messages which are abusive, offensive or defamatory could cause damage to the council's reputation and distress and anxiety to others in the workplace and employees are reminded of their obligations under the Councils Bullying and Harassment policy, Equalities policy and Data Protection policy.

Employees must be aware that if such matters do come to light, disciplinary action may be taken in line with the Council's disciplinary policy. If deemed sufficiently serious, this could result in dismissal.

Security and identity theft

Employees are reminded to be security conscious and take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites and online forums allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords.

Employees must take care when posting such information, in order that it does not allow a breach of security within the Council, or raise the possibility of the employee's identity being stolen.

In addition, employees should:

- Ensure no information is made available that could provide a person with unauthorised access to the Council and/or any confidential information belonging to the Council, councillors, other employees and/or members of the public; and
- Refrain from recording any confidential information regarding the Council, councillors other employees and/or members of the public on any social networking website.

Employees should note that if they are found to have posted confidential material regarding the Council in any format on the online, they are required to assist in any way to ensure such material

is removed without delay. Failure to assist in removing such material in a timely fashion could lead to disciplinary action being taken against that employee.

WHAT IS SOCIAL MEDIA?
Facebook, Twitter, blogs, YouTube, Wikipedia and networking sites such as LinkedIn or IDeA Communities of Practice are all examples of social media. The term covers anything on the internet where content is created and adapted by the people who use the site and which allows two-way conversations.

The Tameside **Social media use: responsible conduct policy** applies to:

- All blogs, wikis, forums, and social networks hosted or sponsored by Tameside;
- Your personal blogs that contain postings about Tameside's business, councillors, employees, residents, customers, or partners;
- Your postings about Tameside's business, councillors, employees, residents, customers, or partners, on any external blogs, wikis, discussion forums, or social networking sites such as Twitter; and
- Your participation in any video related to Tameside's business, councillors, employees, residents, customers, or partners, whether you create a video to post or link to on your blog, you contribute content for a video, or you appear in a video created either by another Tameside employee or by a third party.

WHY DO LOCAL AUTHORITIES NEED SOCIAL MEDIA?
Local authorities and other public sector agencies are increasingly looking to social media to engage with their audiences for two broad reasons:

1. **The audience is changing-** People also expect to 'talk back' when official bodies communicate with them and they expect that those agencies will in turn respond and do so in appropriate language. New media enables that kind of interaction to happen in a more efficient manner than, for instance, arranging regular public meetings. Also our audience is becoming fragmented and diverse in so many ways. The old ways of communicating where budget is invested into a newsletter or another form of mass communication that contains one standard message and assumes this will be effective for everybody is increasingly losing impact. Information needs to be provided in a variety of formats so each target audience can choose how to access it. Photographs can tell a thousand words and videos are very accessible for a wide audience.

2. **Pressure from Central Government -** We all know that public funds are being squeezed from the centre as the focus becomes much tighter on how money is spent, especially on communications. **There** is also an ethos in some areas of Whitehall that egovernment needs to be incentivised and **encouraged**. For these reasons, central government is looking more closely at the degree to which local authorities are using new media to talk to their audiences and this is becoming an increasing factor in the awarding of funds/grants.

WHAT ARE THE BENEFITS OF USING SOCIAL MEDIA?
Used carefully, social media can bring people together over common interests, can be useful for consulting people and getting feedback and publishing information that other media may ignore. However, you must treat social media with respect. Always remember any information or comments you publish on any site (internal or external):

- may stay public for a long time
- can be republished on other websites
- can be copied, used and amended by others
- could be changed to mis-represent what you said
- can attract comments and interest from other people/the media

Always be aware of the standards, conditions of use and guidelines for posting laid down by the owner of any site or network and make sure you comply with them.

USING SOCIAL MEDIA
This policy applies to you participating in any on-line social media (whether listed here or not), whether privately or as part of your role with the Council and sets out the standards of behaviour the Council expects of all its employees.

You are permitted to use social media from a Council computer at work, provided you comply with the Council's Acceptable Use of IT policy, and ensure that you use it in a reasonable manner and unless you are specifically using it to undertake Council business eg consultation with the public that you only engage in such social interaction in your own time.

You must make sure any on-line activity does not interfere with your job, your colleagues, your responsibilities and duties as a Council employee, our commitment to customers, is legal and does not bring the Council into disrepute. If you are found to be in breach of any of these policies, then you may face disciplinary action

STAY LEGAL
You must stay within the law at all times. Be aware that fair use, financial disclosure, libel, defamation, copyright and data protection laws apply on-line just as in any other media. Remember that colleagues and customers may see your online information (eg Facebook.) Whether you identify yourself as an employee of Tameside Council or not, think carefully about how much personal information you want to make public and make sure your profile and the information you post reflects how you want them to see you both personally and professionally.

Never give out personal details like home addresses, phone numbers, financial information or full date of birth to prevent identity theft.

In addition, a person that posts grossly offensive or indecent matter or may be found to be guilty of an offence under the Communications Act 2003.

KEEP IT PRIVATE AND DECENT

Remember your obligations to residents, service users, partners, suppliers and colleagues and to protecting the Council's reputation. Never give out details of or divulge dealings with colleagues, customers or partners without their explicit consent. Check with your manager if you are not sure what is and isn't confidential.

Never make offensive comments about any customer, supplier, partner or any of their employees or your Council colleagues. Don't use ethnic slurs, personal insults, obscenity or behave in ways that would not be acceptable in the workplace. That could bring the Council into disrepute, break the law and leave you open to prosecution and/or disciplinary action.

Don't pick fights, be the first to correct your mistakes and don't alter previous posts without indicatingthat you have done so.

Don't be afraid to be yourself, but be considerate about other people's views, especially around 'controversial' topics such as politics and religion. You can challenge without being abusive.

Be credible, be accurate, fair and thorough and make sure you are doing the right thing.

Share useful information that you gain from using social media with others, where appropriate.

Speaking for the Council
You should not 'speak for the Council' (disclose information, publish information, make commitments or engage in activities on behalf of the Council) unless you are specifically authorised to do so in writing. If you have not been authorised, then please speak to your line manager and the Council's communications team before taking any action.

Remember you are personally liable for what you publish online.

If you are unsure please contact your line manager in the first instance or

- Nicola Smith – Head of Media and Communications
- Tim Rainey – Assistant Chief Executive (Media Marketing and Comms)
- Sandra Stewart – Borough Solicitor/Monitoring Officer
- Paul Turner – Head of Legal Services

GIVING YOUR PERSONAL VIEWS

1. Be professional, responsible and honest and try to add value to any debate. Remember that if people know your **links** with the Council you will be seen as representing the whole Council (even if you are not speaking on our behalf) so be careful.
2. If you are discussing the Council or council-related matters, you must make it clear that you are speaking for yourself and not on behalf of Tameside Council. The easiest way to do this is to write in the 'first person' (I think, my view is..).
3. If you publish any information on a website about the Council or Council-related matters you must include a simple and visible disclaimer such as "The views expressed here are my own and don't necessarily represent the views of Tameside Council"
4. Be aware that you may attract media interest in you as an individual, so be careful whenever you use social media for personal or business reasons. If you have any doubt, speak to your line manager and the Council's communications team before you go on-line.
5. If the media do contact you about something posted on-line, politely ask for their contact details, say you will get back to them and take advice from the Council's communications team before any response is given.

GUIDELINES FOR BLOGGING/BLOGGERS

1. Please see the "Keep it private and decent" section
2. If you already have a personal blog or website which shows in any way in that you work at Tameside Borough Council you must tell your manager. You should include a simple and visible disclaimer such as "The views expressed here are my own and don't necessarily represent the views of Tameside Borough Council"
3. If you want to start blogging, and your blog/website will say that you work for Tameside Council you should tell your manager and use the disclaimer.
4. If you think something on your blog or website may cause a conflict of interest or have concerns about impartiality or confidentiality, speak to your manager. If in any doubt, don't talk about what you do at work – particularly if you work in sensitive areas (such as social work) or on high profile, controversial projects. The Council has to be seen as honest, transparent, fair and impartial at all times. You must not undermine that.
5. If someone offers to pay you for blogging this could cause a conflict of interest and you must consult your manager.

GUIDELINES FOR SOCIAL NETWORKS, DISCUSSION FORUMS, WIKIS ETC

1. Please see the "Keep it private and decent" section
2. Use your best judgment. Remember that there arealways consequences to what you publish.
3. Don't use your Council email account or your email or work number in on-line discussions unless you have been authorised to speak for the Council.
4. It is not a good idea to invite customers to become your friends on social networking sites. There maybe a conflict of interest, security and privacy issues
5. Make sure any wiki entries, articles or comments are neutral in tone, factual and truthful.
6. Never post rude or offensive comments on any online encyclopaedias
7. Before editing an online encyclopaedia entry about the Council, or any entry which might cause a conflict of interest or adding links, check the house rules of the site. You may also need permission from the relevant wiki editor and your line manager.
8. If you edit online encyclopaedias whilst using a work computer, the source of the correction may be recorded as a Tameside Borough Council IP address. That means it may look as if the Council itself has made the changes. If this is correcting an error about the Council,

that's fine – we should be open about our actions. In other circumstances be careful that you do not bring the Council into disrepute through this. If in any doubt, ask the Council's communications team before taking action.

9. We should respond to legitimate criticism with facts but please speak to the Council's communications team for advice before responding; a poor response could make matters worse. Never remove criticism of the Council or derogatory or offensive comments. Report them to the site administrator for them to take action.

GUIDELINES FOR 'MEDIA' SHARING (VIDEO, PHOTOS, PRESENTATIONS)

1. Make sure all video and media is safe to share, does not contain any confidential or derogatory information, and is not protected by any copyright or intellectual property rights.
2. If the content is official Tameside Council content then it must be labelled and tagged as such.
3. Individual work must be labelled and tagged as such. Use a disclaimer where appropriate: "This is my personal work and does not necessarily reflect the views of Tameside Council."

USE OF COUNCIL COMPUTER EQUIPMENT

1. Make sure you have read, understood and signed the Council's Acceptable Use of IT policy. This sets out very clearly what you can and cannot do.
2. You must protect the security of our network and information at all times.
3. Do not install any application.
4. Do not open emails from people you don't know and trust, particularly if they have attachments. Do not forward these within the council unless you know they are virus free.
5. Remember online activity can be traced back to the Council and you. Don't do anything online that breaches the Acceptable Use of IT policy.
6. Do not reveal any details of the Council's IT systems and services, including what software we use for email, internet access and virus protection to minimise the risk of malicious attack.
7. If you use secure systems, such as GovConnect email or to process financial transactions, never log onto social networking sites while connected to those systems. If you have used asocial networking site, please restart your computer before logging onto the secure system to clear any information in the computer's memory cache.

LEGAL ISSUES

Libel

If you publish an untrue statement about a person which is damaging to their reputation they may take a libel action against you. This will also apply if you allow someone else to publish something libellous on your website if you know about it and don't take prompt action to remove it. A successful libel claim against you will result in an award of damages against you.

Copyright

Placing images or text from a copyrighted source (e.g. extracts from publications, photos etc) without permission is likely to breach copyright. Avoid publishing anything you are unsure about or seek permission in advance. Breach of copyright may result in an award of damages against you.

Data Protection

Avoid publishing the personal data of individuals unless you have their express written permission.

Bias and Pre-determination

If you are involved in planning or licensing application or other quasi-judicial decisions, avoid publishing anything that might suggest you don't have an open mind about a matter you may be involved in determining. If not, the decision runs the risk of being invalidated.

Obscene material

It goes without saying that you should avoid publishing anything that people would consider obscene. Publication of obscene material is a criminal offence.

GUIDELINES FOR MANAGERS

Please make sure you and your staff are aware of and working within these guidelines. Please speak to the Heads of Media Marketing and Communications, Legal ICT or Human Resources if you have any questions or concerns about interpreting this policy.

Managers are responsible for deciding what is appropriate, bearing in mind concerns about impartiality, confidentiality, conflicts of interest or commercial sensitivity.

If you believe any employee is breaching these guidelines or is spending too much time on the internet/social media), ask IT to activate internet monitoring for that employee. It is your responsibility as a manager to ensure your staff are not abusing Council IT facilities.

FINALLY....

These guidelines are to protect you and the reputation of the Council they aren't meant to restrict your genuine and work related use of what is an important method of communication and engagement. By its nature though, it is fast and responsive so when a mistake is made it can rapidly get out of control.

If you think social media may help your service you should contact the Head of Media and Communications who can support you and ensure your proposal is supported by the other work being done as part of the corporate communications strategy.

APPENDIX 7

REMOVABLE MEDIA PROTOCOL

1. INTRODUCTION

1.1 This protocol aims to ensure that the use of removable media is controlled in order to maintain integrity of data and to prevent unintended or deliberate adverse impacts to Tameside Metropolitan Borough Council (the Council) information and networks.

1.2 The Council recognises that sometimes there is a business need for information to be accessed or stored outside of the office setting. However, there are risks and requirements associated with this. The Council needs to ensure the correct data is available when required and any information held outside of Council controlled premises is appropriately safeguarded against unauthorised disclosure or loss.

1.3 Removable media refers to devices that are used to store or transport data. In this protocol the term 'removable media' includes but is not restricted to the following;

- Optical Disks (CDs, DVDs);
- USB Memory Sticks (also known as pen drives or flash drives);
- Memory Cards (including Flash Cards, Smart Cards and Mobile Phone SIM Cards);
- Media Card Readers;
- External Hard Drives;
- MP3 Players;
- Digital Cameras; and
- Magnetic/Audio Tapes (including cassettes from Dictaphones and backups).

2. DEFINITIONS

2.1 The following terms are used throughout this document and are defined as follows:

Personal information: is any personal data as defined by the Data Protection Act 1998. Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of personal information held by it as governed by the Data Protection Act 1998.

Sensitive personal information: is any personal information (as defined above) which consists of details relating to their:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- mental/physical health or condition;
- sexual life;
- a committed or alleged offence; and
- details of the proceedings or the sentence of any court.

Protected Information is any information which is;

(a) personal/sensitive personal data *or*
(b) confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way

3. ROLES AND RESPONSIBILITIES

3.1 All those who have access to or use of removable media are responsible for the safety and security of the media and the information stored on them and must ensure they are not compromised whist under their control.

3.2 Any incident where protected information is lost, leaked or put at risk must be reported as a potential security incident. It is the responsibility of all individuals to immediately report any actual or suspected breaches in information security by informing your line manager and/or Risk and Insurance Manager. Failure to do this could result in a loss having more serious consequences than would otherwise have been the case and could result in fines by the Information Commissioner.

3.3 Service areas are responsible for implementing this procedure and must monitor the use of removable media.

4. USE OF REMOVABLE MEDIA

4.1 As set out in the ICT Security Policy, only encrypted USB memory sticks purchased through ICT Services may be used in the Council.

4.2 Purchases of removable media must be done through the Council's approved ordering system. All removable media devices and any associated software must be supplied, configured and installed by authorised Council personnel or a Council approved third party provider.

4.3 Removable media (and the associated software/hardware) must only be used if there is a valid business need and with the approval of a Service Unit Manager or above. Use of removable media to transport protected information outside the office environment should be minimised and used as a last resort when no other method of accessing information is available.

4.4 The only removable media permitted to connect to Council ICT equipment or the Council network is media purchased and approved by ICT Services. Removable media which is not owned by the Council must not normally be connected to Council owned equipment. Exceptionally permission may be granted by a Service Unit Manager or above if there is a strong business case for the connection. Advice from ICT Services should be taken to minimise risk of virus infection and data loss.

4.5 Use of removable media on the Council's network is monitored by ICT Services and unauthorised use will be brought to the attention of managers.

4.6 Any non encrypted device connected to the Council's network will not be permitted to download information onto it and a message will be displayed by the monitoring software. Employees will still be able to view the contents of non-encrypted devices; however it is important that a virus check is carried out on any device that is not provided directly from a trusted source (i.e. ICT Services).

5. SECURITY OF INFORMATION

5.1 Information held on removable media should be a short-term measure. Where relevant, information held on removable media must also remain on the source system or networked computer.

5.2 Where digital information is transferred it is important to remember that at the point it is transferred, it becomes a snapshot of the information at that time. Information temporarily held on removable media should be appropriately labelled to ensure that anyone viewing the information can easily identify the version and its content.

5.3 In order to minimise physical risk such as loss or theft, all removable media must be stored in an appropriately secure and safe environment when not in use (e.g. locked cupboard or drawer).

5.4 Removable media should not be used as the sole storage method for information or to store backup data. If this is the case, please contact ICT Services for advice.

5.5 Anyone using removable media devices to enable work at another site (i.e. home or customer site) must be able to demonstrate that reasonable care is taken during transportation to avoid damage or loss. Removable media should not be used if direct access to the Council network is available at the remote site.

5.6 If any removable media is to be used outside of Council controlled premises, refer to the Mobile and Remote Working Protocol to ensure you are aware of your responsibilities.

5.7 Council issued removable media must not normally be connected to non-Council owned equipment. Exceptionally, permission may be granted by a Service Unit Manager or above if there is a strong business case for the connection. Advice from ICT Services should be taken to minimise risk of virus infection and data loss.

5.8 Passwords needed to access protected information on removable media must only be disclosed to those authorised to access the information held on the media. Passwords must **never** be written down or stored alongside the media.

6. ACCESS TO INFORMATION

6.1 Removable media issued by the Council must only be used for the purposes of Council business. Employees must therefore ensure that any removable media is not accessed by anyone outside the Council without the agreement of a Service Unit Manager.

6.2 Protected information must not be transferred to an external third party (e.g. contractor, partner) via removable media unless this is specified within a relevant Information Sharing Agreement. If removable media is to be used, the security arrangements for the media must also be recorded and reflected within the agreement.

6.3 Should third parties be granted access to Council information, the third party is required to follow this protocol when they use removable media for the purpose of holding or transferring information.

7. SECURE DISPOSAL OF REMOVABLE MEDIA

7.1 It is essential that all removable media is disposed of securely to minimise the risk of the accidental disclosure of sensitive information. All ICT equipment (e.g. USB memory sticks, hard drives etc) that are surplus to requirements or have become damaged must be returned to ICT Services. Where possible, ICT Services will securely wipe removable media for re-use within the Council before considering disposal. For further details on this, refer to the ICT Equipment Disposal/Recycling Policy.

7.2 Tapes can be disposed of using the secure waste bins that are retained by the Benefit Fraud Team. Discs can be carefully snapped in half or shredded (if your shredder is capable) or cut into pieces.

7.3 Removable media devices associated with mobile phones (SIM cards, memory cards etc) should be returned to Media, Marketing and Communications along with the relevant device to ensure any data is removed from the handset before reallocation/disposal.

Employees must be aware that all devices connected to the Council's equipment are monitored ...

APPENDIX 8

MOBILE AND REMOTE WORKING PROTOCOL

1. INTRODUCTION

1.1 All ICT equipment, including portable devices, provided to employees by Tameside Metropolitan Borough Council (the Council) remains the property of the Council and must be returned promptly upon request by ICT Services or by managers for audit and inspection, to enable maintenance work to be undertaken, or for removal or disposal.

1.3 The Council recognises that there are business needs for employees to access and process information outside the office setting. However, there are risks and requirements associated with this. Unfortunately the technology and mobility that make portable devices so useful to employees and the Council can also make them valuable prizes for thieves.

1.4 This protocol applies to any access or use outside Council controlled premises of :

- any ICT Council equipment including mobile telephones, portable devices and static IT equipment; and
- any information held by the Council to which an employee has access because of his or her role within the Council.

Access or use of ICT equipment or information outside Council controlled premises includes non-Council locations such as; an employee's home, premises of another organisation and public venues.

1.5 In this protocol the term 'portable devices' includes but is not restricted to the following:

- Laptop/slate computers;
- Personal Digital Assistants (PDA's);
- BlackBerry's/Smartphones;
- Mobile phones;
- Text pagers;
- Wireless technologies;
- Digital Cameras; and
- Storage devices including flash memory cards/USB memory sticks.

2. DEFINITIONS

2.1 The following terms are referenced throughout this document and are defined as follows;

Mobile Working: Employees who have the ability to work from multiple locations. Usually accompanied by portable computing equipment, employees can utilise any work space at any given time (including home, office, customer sites, Touch Down Points etc.).

Remote Working: Employees who are able to access information or resources from a remote location. This usually applies to workers who perform their work from home or from an alternative office (e.g. Touch-down Points) on an ad-hoc basis.

Home Working: Employees who are based at home or work from home for all or part of the working week on a regular basis. This would be an agreed arrangement and would necessitate the provision of appropriate equipment.

Personal information: is any information about any living individual, who could be identified from the information or any other information that is in the possession of the

Council. The Council is legally responsible for the storage, protection and use of such information as governed by the Data Protection Act 1998.

Sensitive personal information: is any personal information about an individual consisting of details relating to their racial or ethnic origin, their political opinions, religious or similar beliefs, along with mental/physical health or condition and sexual life. Also includes information about a committed or alleged offence, along with the details of the proceedings or the sentence of any court.

Protected Information is any information which is;

(a) personal/sensitive personal data *or*
(b) confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way

VPN (Virtual Private Network): refers to a secure network connection that uses the internet to transmit data. It allows employee's access to the Council network out of the office from a Council issued PC/laptop.

Netilla: works in a similar way to a standard VPN but instead of connecting the PC/laptop to the network, it enables a user to connect from any machine as a remote virtual desktop is created.

WiFi Hotspot: an internet access point in a public location such as a café or hotel.

3. ROLES AND RESPONSIBILITIES

3.1 All employees are responsible for the safety and security of portable devices issued to or used by them. Particular care must be taken when moving equipment between sites, good care must taken of all ICT equipment provided to them wherever it is situated.

3.2 All employees with a Council issued portable device have the responsibility for the information held on the device. Employees must be aware of their surroundings and take appropriate measures when viewing information on a portable device to ensure it is not within view of others.

3.2 It is the responsibility of individuals to immediately report any actual or suspected breach in information security by informing your line manager and/or the Risk and Insurance Manager. Any incident where protected information is lost, leaked or put at risk must be reported as a potential security incident. Failure to do this could not only result in reputational damage, but fines could also be imposed by the ICO.

3.3 Where the Council provides a laptop computer to an employee, it is the responsibility of the user to ensure that the anti-virus updates are maintained by regularly connecting the device directly to the Council network. This can be done by connecting via a designated Touch-down Point or from their office within a Council building and any automatic update should be downloaded. If employees are not clear on how to check if their anti-virus files are up to date refer to the Service Portal 'how to guides' which can be accessed via the home page of the intranet.

3.4 Portable devices may be used for personal purposes by employees so long as it is in accordance with Acceptable Use Guidelines. However, the Council owned equipment must not be used to undertake any private business enterprise.

4. PORTABLE DEVICES

4.1 Access to a Council owned portable device will be authorised by the employee's manager on an individual basis to support the delivery of service provision. All equipment used to store or access any protected information must be supplied, configured and installed by the Council or a Council approved third party provider.

4.2 Employees must not install any software or connect any hardware to a Council owned portable device without the prior permission of the Council. However connection to the following is permitted:

- an external monitor or projector;
- equipment supplied, owned or configured by the Council;
- internet connection via a home router or home broadband modem (wired or wirelessly connected); and
- A printer.

4.3 Users must not update or change the security configuration of any Council portable device unless advised by ICT Services. This is to prevent potential loss of protected information or damage to a portable device.

4.4 To reduce the risk of unauthorised access whilst working out of the office, protected information must only be stored on Council issued portable devices if they are encrypted. Some items like digital cameras cannot be encrypted, however if the contents would be considered to be protected information, the camera (or other storage medium) must be kept securely until it can be transferred to a more secure storage format.

4.5 Any equipment supplied by the Council may only be used by authorised persons. Employees must therefore ensure that the supplied equipment is **not** used by anyone outside the Council. Access to protected information by anyone outside the Council would have to be agreed by a Service Unit Manager. There are instances where permissions may not be required, i.e. showing a Service User information being created about them. However, in this case your Manager should be aware of what you are doing.

4.6 All faults or requests for upgrades must be logged via the ICT Service Portal (available from the home page of the intranet).

4.7 Portable devices issued by the Council are usually insured when they are inside the United Kingdom, although misuse or inadequate protection may invalidate that insurance cover. Employees must seek advice from the Risk and Insurance Team before taking any Council owned portable device outside the United Kingdom as the device may not be covered by the Council's normal insurance against loss or theft. There is also the possibility that the device may be confiscated by Airport Security staff, which could result in having to leave them behind, or they may request to see the contents, which could result in a breach of this policy and possibly the law if the device contains protected information.

5. PHYSICAL SECURITY

5.1 Employees should be aware of the physical security risks associated with working from a remote office or mobile working location. All protected information (including information stored on portable devices and in paper files) must not be left where it would attract the interest of an opportunist thief. Protected information must be located securely and out of sight so that visitors or family members do not have access. Unauthorised disclosure of protected information is a breach of this protocol and the law.

5.2 Council equipment and protected information must be kept safely and securely at all times. When equipment/protected information are at home, employees must:

- ensure that only the employee has access to the equipment/information;
- ensure that the equipment/information is safely and securely locked away when not being used;
- prevent access to the Council equipment and protected information, by family members and visitors; and
- ensure that any telephone conversations discussing protected information cannot be overheard.

These precautions are necessary to reduce the risk of unauthorised persons listening to or viewing Council information.

5.3 Employees who regularly work at home must have a suitable workstation where these issues have been considered. Documents should be collected from printers as soon as they are produced and not left where they can be casually read in order to prevent a potential breach.

6. USE OF INFORMATION OUT OF THE OFFICE

6.1 All Council supplied laptops (and all USB memory sticks authorised for use by the Council) are encrypted and so provide a secure method in which to save information when necessary. However, whilst this is likely to prevent unauthorised access to the information, it does not protect the information against loss. Therefore documents and files should be saved on a shared drives as soon as possible to prevent any loss of information. Once the information is no longer required on the portable device it should be deleted.

6.2 It is also possible to synchronise folders so that they can be worked on off-line, which means there is a local copy of the data. This will allow a user to work out of the office without access to the Council network. However, the use of this is prohibited where the folders contain personal data.

6.3 Where possible, any user working out of the office should be given secure access to the Council network via a Virtual Private Network (VPN) connection. If employees do not have VPN access to the Council network, information may need to be accessed via an authorised mobile device or transferred to a form of removable media to assist mobile and remote working. If the information is of a protected nature, it is essential that the media or device has been issued by the Council and is encrypted and your line manager **must** be aware of what you are doing.

6.4 When working out of the office, employees should **not** be using externally provided WiFi Hotspots or free WiFi connections provided by retail outlets, coffee shops and the like. Even if using a VPN connection supplied by the Council, hackers could still gain access to a connection and may be able to intercept transmissions potentially revealing protected information or password and login details. The only exception to this would be a private network that requires a password to access. For example WiFi at another Local Authority building, or at a business or academic premises. Purchased connectivity at a hotel, where you are given a unique password would also be acceptable.

6.5 Some services may require physical documentation (e.g. paper files) to be removed from the office to assist with mobile and remote working. If this is the case, a booking out system should be in place which meets the requirements of the service. This is to ensure that your Manager is aware of the movement of information within their service, as if a loss occurs they will need to provide assurance they were controlling their information adequately.

6.6 Arrangements must be made to properly dispose of any protected information used out of the office in order to prevent unauthorised access. To do this any information that would qualify as being personal or sensitive must be returned to the Council office and disposed of in the blue Iron Mountain security bins or shredded.

7. NON-COUNCIL EQUIPMENT

7.1 Personal or any other non-Council equipment must not be used to conduct official Council business. This would include employees own smartphones (including iPhones), laptops, iPads/slate PCs, personal desktop computers or internet cafes. However, if an employee has been provided with Netilla access by ICT Services, work may be undertaken within the virtual environment only. Council information cannot be stored or downloaded onto any non-Council equipment outside of Netilla, as it then becomes insecure.

7.2 Some employees will have access to OWA (Outlook Web Application) With Exchange 2010 we have support for WebReady Document Viewing, which will enable employees to view the most common file types within OWA rather than opening another application such as Word which involves saving a copy of the attachment to the computer and potentially caching a copy of the document onto the device being used.

7.3 The setting up of personal iPhones or smartphones to receive "push" emails from an employees' own Council outlook account must **not** be undertaken. If an employee wishes to use their own device for work purposes the procedure in the Personal Device Policy needs to be followed. Also, Council emails must **not** be forwarded on to a personal email account. Emails sent in these ways exit the Council's network and are transmitted over an untrusted network. If an email or attachment containing protected information is sent to a personal device/email account, the contents are open to misdirection, interception and corruption and therefore this would be in breach of this protocol.

7.4 Employees must not install any Council owned/licensed software onto personal equipment, unless this has been authorised by ICT Services. Any software purchased by the Council is licensed to the Council and any unauthorised use outside of the licence is likely to be a breach of copyright and could result in a prosecution.

7.5 Non-Council owned portable devices including mp3 players, iPods/iPhones, cameras and USB memory sticks must **not** be physically connected to Council owned equipment unless they have complied with the requirements of the Personal Device Policy. For further information on this, refer to the Removable Media Protocol. The connection of unencrypted devices is logged and monitored by ICT and downloads to these devices are prevented.

APPENDIX 9

RETENTION AND DISPOSAL GUIDELINES AND SCHEDULE

1. INTRODUCTION

1.1 This Retention and Disposal Schedule outlines the framework for the retention and disposal of information held by Tameside Metropolitan Borough Council (the Council).

1.2 In the course of carrying out its various functions and activities, the Council collects and creates a wide range of information which is recorded. These include but are not limited to;

- Letters received from third parties
- Copy letters which have been sent out
- Invoices
- Completed application forms
- Plans/drawings
- Financial records
- Registers
- Contracts/deeds
- Email communications (and any attachments)
- Photographs
- Tape Recordings
- Case files
- Reports

1.3 The above information can be created and retained as physical records or in electronic form.

1.4 This Retention and Disposal Schedule will ensure that the information it holds is:

Retained for as long as it is needed to enable it to operate effectively, to comply with legislation and the requirements of regulators, and to demonstrate accountability to its stakeholders and to the wider society;

Retained for only as long as it is needed, enabling efficient use of space and minimising the overall costs associated with maintaining records.

1.5 The Council's Retention and Disposal Schedule is based on the Local Government Retention Schedule published by the Information and Records Management Society and additional sources including The National Archives and other Local Authorities. Where there are no statutory requirements to retain information, an assessment of business need has been made and some 'best-practice' time periods have been included.

2. DEFINITIONS

2.1 The following terms are referenced throughout this schedule and are fundamental:

Personal information: is any personal data as defined by the Data Protection Act 1998. Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of personal information held by it as governed by the Data Protection Act 1998.

Sensitive personal information: is any personal information (as defined above) which consists of details relating to their:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- mental/physical health or condition
- sexual life
- a committed or alleged offence
- details of the proceedings or the sentence of any court

Protected Information is any information which is;

(a) personal/sensitive personal information *or*
(b) confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way

Document/Record: A document/record provides evidence of the functions, decisions, procedures, operations or other activities of an organisation because of the informational value of their contents. This includes books, papers, maps, photographs, email messages, excel files, letters, memos etc. Within this schedule, the terms document/record will be used interchangeably.

3. ROLES AND RESPONSIBILITIES

3.1 All employees who receive, create, maintain or delete Council records are responsible for ensuring that they do so in accordance with this schedule.

3.2 It is the responsibility of individual Service Areas to carry out the necessary retention and disposal requirements for their records.

3.3 Legal Services can advise on whether minimum retention periods are prescribed by law, and whether retention is necessary to protect the Council's position where the likelihood of a claim has been identified. However, Legal Services staff cannot be expected to possess the operational or background knowledge required to assess whether a particular document may be required by the Service concerned for operational need.

4. RETENTION

4.1 The retention of specific documents may be necessary to:

- Fulfill statutory or other regulatory requirements
- Evidence events/agreements in the case of disputes
- Meet operational needs
- Ensure the preservation of documents of historic or other value

4.2 However, the permanent retention of all documents is undesirable, and can cause a shortage of storage space as well as creating a potential fire risk (physical records) and in some cases the indefinite retention of personal data may be unlawful. Therefore, specified time periods of retention must be followed.

4.3 The retention periods apply to records in all formats regardless of whether they are held on paper, electronically, microfilm or any other storage media.

4.4 While the retention schedule relates to ***primary*** or ***original*** records, it is compulsory to destroy any duplicate/additional/backup copies of the record as retaining information for longer than necessary may breach the Data Protection Act. Additionally, any secondary

copies of a record would have to be released under a Freedom of Information request even if the original had been destroyed.

4.5 The retention periods specified are the minimum requirements. Each retention period in this schedule is the minimum length of time the record must be retained. Once a record has reached the minimum period of retention, it is necessary to review the record to ensure that it can be disposed of or if may need to be retained for a further period of time (e.g. is subject to a FOI request).

4.6 Where a specified retention period is fairly short (1 year or under), Service Areas need to consider whether the records will need to be kept for audit purposes. Auditors will be more concerned with recent records (i.e. current year and previous year) and this may extend the period of time for which a record needs to be retained. For further advice on what records this may apply to, please seek guidance from Internal Audit.

4.7 If the decision is made to store a document or set of documents longer than specified within the retention schedule, consideration should be given the content of the information i.e. all records of personal data must be compliant with the eight principals of the Data Protection Act. Consideration should also be given to the means of storage as some storage mediums are not regarded as acceptable for the long-term preservation of information. If the decision is made to extend a retention period, the record may need to be transferred to an alternative method of storage.

4.8 The decision to retain specific information longer than the minimum retention period should be properly documented in the Extended Retention Authorisation Form.

5. STORAGE AND PRESERVATION

5.1 The storage of information needs to be in a clean, secure and stable environment. Necessary controls need to be put in place to protect from damage, disaster (i.e. fire, water), and theft, as the Council has an obligation to protect this information in any format.

5.2 Storage areas need to be well organised, with all files labelled and indexed as accurately as possible. Service Areas need to be aware of the information held in storage areas and the calculated destruction dates.

5.3 Storage facilities need to be suitable to preserve information in its original state. The documents need to be able to survive the length of time required for the retention requirements. Council employees directly involved with the storage of non-electronic information need to consider the risks to the information (e.g. aging of paper), and review the storage arrangements regularly.

6. DISPOSAL

6.1 The untimely disposal of documents could cause the Council:

- Difficulty in defending litigious claims
- Operational problems
- Failure to comply with the Freedom of Information or Data Protection Acts

6.2 The method of disposal will largely depend on the format of the information. Council records must be disposed of using one of the following methods:

- Confidential waste – *i.e.* red bin's within the Council offices
- Physical disposal on site (paper records - shredding)
- Hard Deletion or 'scrubbing' – where computer files are concerned

6.3 Under no circumstances should records containing protected information be simply binned or deposited in the recycling bins. To do so could result in the unauthorised disclosure of such information and render the Council liable to prosecution or other enforcement action under the Data Protection Act. Such documents must be destroyed securely, e.g. by physical disposal or placed in the red confidential waste bins.

6.4 It is important that the disposal of records happens as part of a managed process and that it is adequately documented. Details of the document being disposed of; the date and method of disposal, and the officer who authorised disposal should all be recorded within the Record Disposal Authorisation Form. All Record Disposal Authorisation forms should be retained permanently to evidence the appropriate disposal of records. This is particularly important due to the Freedom of Information Act (FOIA), to confirm we no longer hold applicable information.

6.5 The disposal of records should be suspended if the records become the subject of a Freedom of Information request in order to consider disclosure as usual. Deliberate disposal of relevant records in such cases could involve the criminal offence of obstructing or perverting the course of justice. A court is also likely to draw adverse inferences from such an exercise and it is unlikely that a court would be satisfied with any explanation for deliberate record disposal after the commencement of proceedings.

6.6 If a record due for disposal becomes the subject of a request, disposal should be delayed until disclosure has taken place or, if the decision is not to disclose the information, until the complaint and appeal provisions of the FOIA have been exhausted. If the information was disclosed, the request may indicate that there is some wider interest in the matter and that the appropriateness of the disposal should be reconsidered. In this case, a further review will be required and the information may need to be retained for a further short period before disposal.

7. RETENTION / DISPOSAL SCHEDULE

7.1 Any decision whether to retain or dispose of a document should be taken in accordance with this schedule. The schedule consists of:

The **Retention Table** contained in Appendix 1. This provides guidance on the minimum retention periods for specific classes of documents/records.

The **Extended Retention Authorisation Form** is to be completed if a record is to be retained longer than the stated period. This must be attached to the record so that anyone handling the record is aware of the requirements for storage.

The **Record Disposal Authorisation Form** must be completed before any document can be disposed of. The forms must be retained permanently to evidence the appropriate disposal of records. This is particularly important due to the Freedom of Information Act (FOIA), as it helps to confirm we no longer hold applicable information.

8. GENERAL RECORDS

8.1 There are some records that do not need to be kept and may be routinely destroyed in the normal course of business as they are either low-value or of short-term use. This includes;

- 'With compliments' slips
- Catalogues and trade journals
- Telephone message slips
- Non-acceptance of invitations

- Trivial electronic mail messages or notes that are not related to Council business
- Requests for stock information such as maps, plans or advertising material
- Out-of-date distribution lists
- Draft copies which lead to a final report

8.2 Duplicated and superseded material such as stationery orders, manuals, forms, address books and reference copies of reports may also be destroyed under this rule. Electronic copies of documents where a hard copy has been printed and filed, and fax receipts after filing a photocopy, can also be destroyed.

8.3 This should NOT be applied to records or information that can be used as evidence (i.e. to prove that something happened). Each service should have its own protocol which clearly sets out what records it wishes to keep in its systems to support its business.

APPENDIX 9

Appendix 1 - Retention Table

Please use links below to take you to the appropriate record on the retention table.

Adult Care Services
- Asylum seekers
- Carers
- Community support
- Criminal justice
- Residential homes
- Social issues
- Supporting adults
- Supporting disabilities

Children and families services
- Adoption and fostering
- Child protection
- Childminding
- Children looked after in care
- Communications
- Programme management and development
- Residential homes
- Social issues
- Special education
- Supporting children
- Supporting disabilities
- Training
- Youth justice
- Youth services

Community safety and emergencies
- Advice
- Community safety
- Emergency planning
- Emergency service
- Enforcement
- Fire prevention
- Measures against vandalism
- Training

Consumer affairs
- Advice
- Enforcement
- Environmental health
- Investigation, inspections and monitoring
- Registration, certification and licensing

Council property
- Common land
- Maintenance of council property
- Property acquisition and disposal
- Property and land management
- Property use and development

Crematoria and cemeteries
- Burial identity and location
- Maintenance of burial grounds

Democracy
- Decision making
- Executive
- Governance
- Honours and awards
- Member support
- Planning
- Representation

Economic development
- Business intelligence
- Promotion
- Regeneration
- Sustainability
- Tourism
- Training

Education and skills
- Access and inclusion
- Admissions and exclusions
- Advice
- Arts services
- Curriculum development
- Education welfare
- Employment skills
- Life long learning
- Management of schools
- Teaching

Environmental protection
- Advice
- Conservation
- Monitoring

Finance
- Accounts and audit
- Asset management
- Financial provisions management
- Financial transactions management
- Local taxation
- National taxation
- Payroll and pensions

Health and safety
- Community safety
- Compliance
- Monitoring
- Risk management

Housing
- Advice
- Enforcement
- Estate management
- Housing provision
- Housing stock
- Managing tenancies

APPENDIX 9

Human resources
. Administering employees
. Employee relations
. Equal opportunities
. Monitoring employees
. Occupational health
. Recruitment
. Terms and conditions of employment
. Training
. Workforce planning

Information and communication technology
. Infrastructure
. System support

Information management
. Access to information
. Archives
. Knowledge management
. Records management
. Registration

Legal services
. Advice
. Bylaws
. Land registration
. Land and highways
. Litigation
. Management of legal activities
. Planning controls

Leisure and culture
. Allotments
. Archives
. Arts
. Community facilities
. Leisure promotion
. Libraries
. Museums
. Parks and open spaces
. Sports facilities
. Sports
. Tourism

Management
. Ceremonial
. Communication support
. Corporate communication
. Enquiries and complaints
. External audits
. Preparing business
. Project management
. Quality and performance
. Statutory returns
. Strategic planning

Planning and building control
. Building control
. Covenant control
. Development control
. Forward planning

Procurement
. Contracting
. Market information
. Tendering

Registration and coroners
. Inquiries into deaths
. Marriage services
. Registration of births, marriages and deaths
. Treasure trove

Risk management and insurance
. Claims
. Insuring against loss
. Risk management

Transport and infrastructure
. Design and construction
. Harbours and waterways
. Highway development control
. Highway enforcement
. Infrastructure management
. Public transport
. Rights of way
. Road maintenance
. Road safety
. School transport
. Traffic management
. Transport planning

Waste management
. Fly tipping
. Street cleaning
. Waste collection
. Waste disposal
. Waste reduction

Record Title	Description	Scope	Retention Period	Rationale
Adult Care Services				
Asylum Seekers				
Advice and Support		Information on temporary accommodation, meals and other advice and support for asylum seekers	DESTROY – 2 years from last contact	Records Management Society of Great Britain
Nationality Checking		Checking applications for British Citizenship to ensure all the paperwork is correct before the application is submitted to the Home Office	DESTROY – 2 years from last contact	Records Management Society of Great Britain
Carers				
Agency Provided Services	Case Files - carer	Information concerning our use of 'agency' care provisions	DESTROY – 25 years after end of employment	Thurrock Council
Assessment	Case Files – carer	Assessment of suitability of a carer, information about carers' identity, history etc…	DESTROY – 25 years after end of employment	Thurrock Council
Financial Support	Case Files – carer	Details of financial support provided to carer	DESTROY – 3 years after end of employment	Accounts and Audit Regulations 1974
Legal	Case Files – carer	Any legal issues	DESTROY – 25 years after end of employment	Thurrock Council
Licensing	Case Files – carer	Details of the carer's driving and any other licences	DESTROY – 1 years after end of employment	Thurrock Council
Review	Case Files – carer	Carer reviews	DESTROY – 25 years after end of employment	Thurrock Council
Community Support				
Day Centres		Provision of day centres	DESTROY - 7 years from last contact	Records Management Society of Great Britain
Groups		Information on recognised groups and organisations that provide advice	DESTROY - 7 years from last contact	Records Management Society of Great Britain

		and support for those who may be in need of community care		
Criminal Justice				
Court Orders		Community reparation and community service orders	DESTROY – on expiration of order	Avon and Somerset Police
People on Bail		Support to the courts and to people on bail	DESTROY – 6 years from termination	Staffordshire County Council
Residential Homes				
Operation of Homes	Case Files – Residential Home	Details of home's activities	DESTROY – 25 years from closure	Retention Guidelines for Local Authorities No. 3.25
Operation of Homes	Case Files – Residential Home	Details of home's diary	DESTROY – 25 years from closure	Retention Guidelines for Local Authorities No. 3.25
Operation of Homes	Case Files – Residential Home	Details of home's menus	DESTROY – 1 year from closure	Retention Guidelines for Local Authorities No. 3.25
Operation of Homes	Case Files – Residential Home	Record of home's rosters	DESTROY – 25 years from closure	Retention Guidelines for Local Authorities No. 3.25
Registration	Case Files – Residential Home	Any other related information including Care Home's licence details	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 3.24
Social Issues				
Substance Misuse		Work to prevent and action to address drug misuse and related issues	Destroy 7 years from last contact	Records Management Society of Great Britain
Supporting Adults				
Assessment	Case Files – Service User	Assessment of whether applicant is eligible for services and judgements about what services should be provided	DESTROY – 6 years after last contact	Retention Guidelines for Local Authorities No. 3.18
Assessment	Case Files – Service User	Details of assigned carers	DESTROY – 6 years after last contact	Retention Guidelines for Local Authorities No. 3.18
Assessment	Case Files –	Contact details for both client and	DESTROY – 6 years after	Retention Guidelines for Local

	Service User	carers	last contact	Authorities No. 3.18
Assessment	Case Files – Service User	May include; name, DOB, gender, address, ethnicity, religion, next of kin and support history of client	DESTROY – 6 years after last contact	Retention Guidelines for Local Authorities No. 3.18
Catering Services	Case Files – Service User	Management of catering facilities within social care	DESTROY – 6 year from date of closure	Staffordshire County Council
Finance and Commissioning	Case Files – Service User	Information relating to any financial support provided Accounting information should go under 'finance'	DESTROY – 8 years after provision of support ended	Thurrock Council
Grants	Case Files – Service User	Grants applied for client	DESTROY – 8 years after provision of support ended	Thurrock Council
Health	Case Files – Service User	The clients health details	DESTROY – 8 years after provision of support ended	Thurrock Council
Legal	Case Files – Service User	Details of any legal issues	DESTROY – 8 years after provision of support ended	Thurrock Council
Licensing	Case Files – Service User	The Issue of Blue Badge Disabled Parking Permits (formally known as orange badges) for this individual	DESTROY – 3 years after provision of support ended	Thurrock Council
Looked after in care	Case Files – Service User	Details of any residential care	DESTROY – 8 years after provision of support ended	Thurrock Council
Mental Health	Case Files – Service User	Any details about the clients mental health	DESTROY – 10 years after provision of support ended	Retention Guidelines for Local Authorities No. 3.17
Occupational Therapy	Case Files – Service User	Details of any occupational therapy received	DESTROY – 8 years after provision of support ended	Thurrock Council
Referral	Case Files – Service User	Request for service or service transferred to another provide	DESTROY – 8 years after provision of support ended	Thurrock Council
Review	Case Files – Service User	Details of any review of services	DESTROY – 8 years after provision of support ended	Thurrock Council
Transport Services	Case Files – Service Providers	Provision of transport	DESTROY – 7 years after last contact	Thurrock Council
Supporting Disabilities				
Deaf		Support for the deaf in communicating with those who can	DESTROY – 6 Years from last contact	Records Management Society of Great Britain

		hear		
Employment		Advice and support on training and employment	DESTROY – 6 Years from last contact	Records Management Society of Great Britain
Equipment Advice		Advice on purchase and/or loan of specialist equipment	DESTROY – 6 Years from last contact	Records Management Society of Great Britain
Independence at home		Rehabilitation, advice to regain independence in the home or the provision of aids	DESTROY – 6 Years from last contact	Records Management Society of Great Britain
Personal transport		Information on the Mobility scheme	DESTROY – 6 Years from last contact	Records Management Society of Great Britain
Children and Families Services				
Adoption and Fostering				
Adoptive Parent	Case Files - Carer	Information about adoptive parents	DESTROY – 100 years from date of adoption	Adoption and Children Act 2002 ss. 56-65; The Disclosure of Adoption Information (Post-Commencement Adoptions) Regulations 2005
Assessment	Case Files – Carer	Assessment on the suitability of a carer	DESTROY – 25 years from termination	Retention Guidelines for Local Authorities No. 3.4
Financial Support	Case Files – Carer	Information about financial support	DESTROY – 3 years after end of financial year	Accounts and Audit Regulations 1974
Foster Carer	Case Files – Carer	Information that is foster care related	DESTROY – 10 years from provider status ceases, 3 years from date of refusal or withdrawal EXCEPT – 75 years if concerns over circumstances	Fostering Services Regulations 2002 reg.32
Legal	Case Files – Carer	Legal issues	DESTROY – Fostering – 10 years from termination of last placement Adoption – 100 years from date of adoption	The Fostering Services Regulations 2002 No. 57; Adoption Agencies Regulations 2005 No. 389
Licensing	Case Files – Carer	Care or care licence	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 9.18

Review	Case Files - Carer	Details of reviews of the carer	DESTROY –10 years from termination of last placement	The Fostering Services Regulations 2002 No. 57
Child Protection				
Case assessment	Case files – child protection	Process involving individual case assessment	DESTROY – 23rd birthday or 5 years from date of death	Arrangements for Placement of Children (General) Regulations 1991 No 890
Case assessment	Case files – child protection	Process involving initial assessment and advice	DESTROY - 10 years from creation	Foster Placement (Children) Regulations Statutory Instrument 1991 No. 910
Registration		Consolidated listing of children requiring protection	DESTROY – 23rd birthday or 5 years from date of death	Arrangements for Placement of Children (General) Regulations 1991 No. 890
Schedule 1 Offenders		Consolidated listing of section 1 offenders	PERMANENT – Retain for 70 years then offer to archivist	Retention Guidelines for Local Authorities No. 3.7
Childminding				
Registration		Provision of a list of registered childminders	DESTROY – 6 years from date of creation	Staffordshire County Council
Support for childminders		Information and support for those interested in becoming a registered childminder and those already registered	DESTROY – 6 years from date of creation	Staffordshire County Council
Children Looked After in Care				
Registration		Consolidated list of children looked after in care	DESTROY – 23rd birthday or 5 years from date of death	Arrangements for Placement of Children (General) Regulations 1991 reg. 10
Communications				
Complaints		Complaint records	DESTROY – 10 years after complaint dealt with	Arrangements for Placement of Children (General) Regulations 1991
Programme Management and Development				
Services for Children		Process involved in development of services or programmes for children	DESTROY – 7 years from closure	Retention Guidelines for Local Authorities No. 3.20
Supporting Children		Process involved in provision of services or programmes to support	DESTROY – 25 years from closure	Retention Guidelines for Local Authorities No. 3.21

		the development of children		
Supporting Young Persons		Process involved in provision of services or programmes to support the development of young persons	DESTROY – 15 years from closure	Retention Guidelines for Local Authorities No. 3.22
Supporting Adults		Process involved in provision of services or programmes to adults	DESTROY – 7 years from closure	Retention Guidelines for Local Authorities No. 3.23
Residential Homes				
Operation of homes	Case files – residential homes	Documentation about the running of a children's home (information about individual clients must go on the individual child file)	DESTROY – 15 years from date of last entry	Children's Homes Regulations 2001 reg. 29
Operation of homes	Case files – residential homes	Information about activities in the home	DESTROY – 15 years from date of last entry	Children's Homes Regulations 2001 reg. 29
Operation of homes	Case files – residential homes	The home's diaries, or listing of daily occurrences within the home	DESTROY – 15 years from date of last entry	Children's Homes Regulations 2001 reg. 29
Operation of homes	Case files – residential homes	Menu information	DESTROY – 1 year from date of last entry	Children's Homes Regulations 2001 reg. 29
Operation of homes	Case files – residential homes	Roster sheets and arrangements	DESTROY – 15 years from date of last entry	Children's Homes Regulations 2001 reg. 29
Registration	Case files – residential homes	Children's home register	PERMANENT – 15 years from date of last entry	Children's Homes Regulations 2001 reg. 29
Social Issues				
Substance Misuse		The use of drugs for non medical purposes including drug abuse and addiction	Destroy - 10 years from last contact	Essex County Council
Special Education				
Learning Support		Educational arrangements for those with learning difficulties, and support for other special cases e.g. talented or gifted children, or those	DESTROY – 35 years from closure	Retention Guidelines for Local Authorities No. 3.13

		disadvantaged by language or gender		
Supporting Children				
Admission appeals	Case files - child	Information in regard to appeals on admission to a specific school	DESTROY – 25 years from last action	Staffordshire County Council
Adoption process	Case files – child	Information about adoption	DESTROY – 100 years from date of adoption	Adoption and Children Act 2002 ss. 56-65; The disclosure of Adoption Information (Post - Commencement Adoptions) Regulations 2005
Advice	Case files – child	Help given to assist an individual child	DESTROY – on child's 21st birthday	Thurrock Council
Assessment	Case files – child	Assessment whether applicant is eligible for services or judgement about what service should be provided	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Assessment	Case files – child	Choice of services offered and action to be taken	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Assessment	Case files – child	Details of involved carers	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Assessment	Case files – child	Details of contact details for family/child and care staff	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Assessment	Case files – child	May include; name, DOB, gender, address, ethnicity, religion, next of kin and support history	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Attendance and truancy	Case files – child	Children not attending school	DESTROY – 3 years from date of last entry	The Education (Pupil Registration) Regulations 1995 No 2089
Child protection	Case files – child	Any information concerning protection of the child or children	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Children's rights	Case files – child	Information relating to children	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Arrangements for Placement of Children (General) Regulations 1991 reg. 9

Continuing Care	Case files – child	Details relating to the client as a student	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Continuing Care	Case files – child	Student profile details	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Continuing Care	Case files – child	Details about any work experience offered or undertaken	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Educational achievement assessments	Case files – child	Education history	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Education psychology	Case files – child	Assessing children for special educational need and assisting children who may need counselling as a result of an incident	DESTROY – 35 years from closure	Retention Guidelines for Local Authorities No. 3.13
Educational Welfare	Case files – child	Information relating to education welfare issues	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Finance and commissioning	Case files – child	Details about any commissioned services, accounting information goes under 'Finance'	DESTROY – 3 years after end of financial year	Accounts and Audit Regulations 1974
Financial Support	Case files – child	General information about financial support provided, accounting information goes under 'finance'	DESTROY – 3 years after end of financial year	Accounts and Audit Regulations 1974
Financial Support	Case files – child	Clothing grants provided	DESTROY – 3 years after end of financial year	Accounts and Audit Regulations 1974
Financial Support	Case files – child	Meals provided for pupils within schools	DESTROY – 3 years after end of financial year	Accounts and Audit Regulations 1974
Financial Support	Case files – child	Any student awards made	DESTROY – 3 years after end of financial year	Accounts and Audit Regulations 1974
Financial Support	Case files – child	Student loans provided	DESTROY – 3 years after end of financial year	Accounts and Audit Regulations 1974
Financial Support	Case files – child	Information relating to travel passes	DESTROY – 3 years after end of financial year	Accounts and Audit Regulations 1974

Fostering process	Case files – child	Details about the management of the client's foster care	DESTROY – 10 years after termination of foster carer	The Fostering Services Regulations 2002 No. 57
Grants	Case files – child	Details about other grants	DESTROY – 3 years after end of financial year	Accounts and Audit Regulations 1974
Health	Case files – child	Details of any health issues	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Hospital and home tuition	Case files – child	Tuition for sick children and pregnant school girls in the home or hospital environment	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Legal	Case files – child	Details relating to legal issues	DESTROY – on child's 21st birthday	Retention Guidelines for Local Authorities No. 3.3
Licensing	Case files – child	Details of any licences for a child to take part in performing arts, sports or modelling activities, work or similar	REVIEW – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Looked after children in care	Case files – child	Information about any residential care arrangements	DESTROY – 75th anniversary of the child's birth or 15 years after death if the child dies before age 18	Children's Home Regulations 2001 reg.28
Referral	Case files – child	Request for service or service transferred to another provider	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Review	Case files – child	Details of any care reviews	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
School exclusions	Case files – child	Permanent or temporary exclusion from school	DESTROY – 25 years from last action	Retention Guidelines for Local Authorities No. 3.19
Special educational needs	Case files – child	Educational arrangements for those with learning difficulties, and support for other special cases e.g. talented or gifted children, or those disadvantaged by language or gender	DESTROY – 35 years from closure	Retention Guidelines for Local Authorities No. 3.13
Supporting Disabilities				

Deaf		Supporting communication for the deaf	DESTROY – 75th birthday – or 15 years after death if child dies before 18	Care Planning, Placement and Case Review (England) Regulations 2010 No. 959
Training				
Support training		Training provided to support individuals or organisations working with or for clients	DESTROY – 25 years from termination	Retention Guidelines for Local Authorities No. 6.3
Youth Justice				
Case management	Case files	Youth offending teams with dealing with young people who have offended and youth teams dealing with preventing youth crime and supporting young people at risk	DESTROY – 25 years from DOB or 10 years from last contact	Retention Guidelines for Local Authorities No. 3.12
Youth Services				
Youth service provision		Includes youth clubs and voluntary youth organisations as well as services provided to young people by statutory bodies	DESTROY – 25 years from DOB or 10 years from last contact	Retention Guidelines for Local Authorities No. 3.12
Community Safety and Emergencies				
Advice				
Contingency planning		Activities to provide advice on contingency planning to business	DESTROY – 2 years after advice superseded	Thurrock Council
Fire safety planning		Activities relating to the provision of Fire Safety services	DESTROY – 3 years from date of creation	Lincolnshire County Council
Home security		Specific, immediate and practical security advice to householders	DESTROY – 3 years from date of creation	Lancaster City Council
Community Safety				
CCTV surveillance		CCTV related information	DESTROY – 31 days from date of recorded unless required for legal purposes	Lincolnshire County Council
Community wardens	Nominations and Appointments	Information on actions of community wardens. Including information shared with police and other agencies	DESTROY – Once obsolete	Eastbourne Borough Council
Crime reduction		Activities designed to reduce the	PERMANENT – Offer to	Association of Chief Police Officers

		impact and fear of crime	archivist	in Scotland (ACPOS) Retention Schedule
Neighbourhood watch		Council involvement in neighbourhood watch schemes	DESTROY – 6 months from date of receipt	Avon and Somerset Police Retention Schedule
Emergency Planning				
Emergency agencies		List of public contact s for emergency agencies	DESTROY when superseded	Lincolnshire County Council
Emergency call – outs		List of council contact numbers to use in the case of any emergency or major incidents	DESTROY – 6 years from conclusion of incident	Avon and Somerset Police Retention Schedule
Emergency calls – 999		Process around receipt and despatch of emergency vehicles	DESTROY – 6 years from conclusion of incident	Avon and Somerset Police Retention Schedule
Emergency plan		Documents containing council's plans and procedures for dealing with emergencies	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 9.11
Emergency plan		Information on tests of the emergency plan	DESTROY – 10 years after closure	Retention Guidelines for Local Authorities No. 9.12
Emergency warnings		Weather, security, incident warnings etc… made to the public	DESTROY – 2 years after matter is concluded	Retention Guidelines for Local Authorities No. 9.19
Emergency Service				
Notifications		The process of notification to individuals and organisations on their failures to conform to licensing standards (legislation in regard to emergency services)	DESTROY – 2 years after matter is concluded	Retention Guidelines for Local Authorities No. 9.19
Special service provision		Saving cats from trees, unlocking doors, car accidents etc…	DESTROY – 5 years from last action	Records Management Society of Great Britain
Enforcement				
Fire safety legislation		Enforcement of fire safety legislation	DESTROY – 2 years after matter is concluded	Retention Guidelines for Local Authorities No. 9.19
Fire safety legislation		Prosecutions for breach of fire safety legislation	DESTROY – 7 years after last action	Police and Criminal Evidence Act 1984
Fire Prevention				
Fire certification		Documentation relating to applications from organisations for	DESTROY – 12 years after expiry or when superseded	The National Archives Retention and Disposal Guidance 1.

		the granting of fire certificates		
Fire hydrant inspections		Fire hydrant inspection records	DESTROY – 7 years after last action	Retention Guidelines for Local Authorities No. 9.20
Fire safety		Advice given to individuals and organisations on an individual basis relating to fire safety and emergencies	DESTROY – 2 years after advice superseded	Retention Guidelines for Local Authorities No. 9.13
Fire safety inspections		Fire safety inspection records	DESTROY – 7 years after last action	Retention Guidelines for Local Authorities No. 9.14
Incident monitoring		Incident reports and frequency monitoring	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 9.20
Incident monitoring		Incident reports and frequency monitoring	DESTROY – 7 years after closure	Retention Guidelines for Local Authorities No. 9.20
Inspections		Other fire safety information	DESTROY – 7 years after last action	Retention Guidelines for Local Authorities No. 9.20
Investigations		Fire safety investigation records	DESTROY – 7 years from last action	Records Management Society of Great Britain
Measures Against Vandalism				
Fly posting		Removal of illegally posted advertisements, leaflets and similar items	DESTROY – 6 years from last action	Eastbourne Borough Council
Removal of graffiti		Information reporting on the removal of graffiti	DESTROY – 6 years from last action	Eastbourne Borough Council
Training				
Training exercises		Training exercises for major incidents and fire services	DESTROY – 10 years after closure	Retention Guidelines for Local Authorities No. 9.12
Consumer Affairs				
Advice				
Campaigns		Information relating to campaigns within consumer affairs	DESTROY – 6 years after creation	Limitation Act 1980
Enforcement				
Prosecution of offences	Case files - organisation	Documentation relating to enforcement action on dangerous and wild animals	DESTROY – 7 years from investigation complete	Records Management Society of Great Britain

Prosecution of offences	Case files – organisation	Documentation relating to enforcement action on health and safety in the workplace	DESTROY – 7 years from investigation complete	Records Management Society of Great Britain
Prosecution of offences	Case files – organisation	Inspections of premises, individuals or organisations carried out	DESTROY – 7 years from investigation complete	Records Management Society of Great Britain
Prosecution of offences	Case files - organisation	Documentation relating to enforcement action on weights and measures	DESTROY – 7 years from investigation complete	Records Management Society of Great Britain
Environmental Health				
Animal control		Information related to the environmental health function. Information on activities to reduce the risk to human health from domesticated animals and/or the premises where they are kept, to prevent nuisance from pet animals and to reduce the risk to animal health arising from commercial keeping of pet or similar non livestock animals	DESTROY – 2 years from last action	Nottingham City Council
Investigation, inspections and monitoring				
Inspection	Case files – organisation	Inspection of premises, individuals or organisations carried out	DESTROY – 6 years after disposal of the equipment	Records Management Society of Great Britain
Inspections	Case files – organisation	Documentation regarding inspections made on establishments concerning food hygiene standards	DESTROY – 7 years after inspection	Records Management Society of Great Britain
Investigations	Case files – organisation	Process of investigation of a possible infringement in this area	DESTROY – 7 years from last action	Records Management Society of Great Britain
Investigation	Case files – organisation	Investigations and reports on complaints regarding animals	DESTROY – 7 years from last action	Records Management Society of Great Britain
Monitoring	Case files – organisation	The process of monitoring various aspects within this area	DESTROY – 7 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring concerning pollution of the air	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files –	Monitoring of the health and well	DESTROY – 3 years from	Retention Guidelines for Local

	organisation	being of animals	last action	Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring of food hygiene	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring of food hygiene within home care programmes	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	The monitoring of food safety	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring of food standards	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring of hazardous substances	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring of pollution of land	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring the spread and containment of pollution	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring the quality and safety of private drinking water supplies	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring the contamination of rivers	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring of business and industry	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring of swimming pool safety and hygiene standards	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring and regulation of product safety	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring of infectious diseases	DESTROY – 7 years from last action after considering retention	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring of consumer affairs response	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 9.3
Monitoring	Case files – organisation	Monitoring of general nuisance within the public domain	DESTROY – 3 years from last action	Environmental Protection Act 1990
Registration, Certifications and Licensing				
Entertainment and drinks		Consolidated listing of licensed entertainment and drink venues	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16

Food premises		Consolidated listed of licensed food premises	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
License premises		Consolidated listing for the sale or consumption of alcohol	DESTROY – 3 years after creation	Licensing Act 2003
Licensing	Animal boarding licences	Documentation involved with licensing of animal boarding establishments	DESTROY – 2 years after registration lapses	Animal Boarding Establishments Act 1963
Licensing	Animal breeding licences	Documentation involved with licensing of animal breeding	DESTROY – 2 years after registration lapses	Breeding of Dogs Acts 1973 and 1991; Breeding and Sale of Dogs (Welfare) Act 1999
Licensing	Auction premises licences	Documentation involved with licensing of auction premises	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Building materials licences	Documentation involved with licensing of building material	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Caravan and campsite licences	Documentation involved with licensing of meat retailers	DESTROY – 2 years after registration lapses	Caravan Sites and Control of Development Act 1960; Caravan Sites Act 1968
Licensing	Cemetery licences	Documentation regarding caravan and camp site licences	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Cooling towers	Documentation relating to the licensing of cemeteries	DESTROY – 2 years after registration lapses	The Notification of Cooling Towers and Evaporative Condensers Regulations 1992
Licensing	Credit licensing	Documentation relating to the licensing of cooling towers	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Crematoria licences	Documentation relating to the licensing of crematoria	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Dangerous wild animal licences	Licensing documentation regarding dangerous wild animals	DESTROY – 2 years after registration lapses	Dangerous Wild Animals Act 1976
Licensing	Entertainment licences	Documentation regarding entertainment licences	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Food business	Licensing documentation regarding food	DESTROY – 2 years after registration lapses	Food Safety Food Premises (Registration) Regulations 1991

	licences			
Licensing	Food licences	Documentation relating to the licensing of food related issues	DESTROY – 2 years after registration lapses	Food Safety Act 1990
Licensing	Hackney licences	Documentation relating to the licensing of Hackney carriages	DESTROY – 2 years after registration lapses	Local Government (Miscellaneous Provisions) Act 1976
Licensing	Highway projection licences	Documentation relating to the licensing of Highway projection	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Hoarding licences	Documentation relating to hoarding licensing	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Infectious diseases licensing and use	Documentation relating to the licensing and use of Infectious diseases	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Late hours catering licences	Documentation relating to late hours catering licences	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Liquor license	Documentation relating to liquor licensing	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Lottery registration	Documentation regarding gambling and lottery licences	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Massage and special treatment licences	Documentation relating to the licensing of massage and special treatment establishments	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Non medicinal poisons licences	Documentation relating to the licensing of non medicinal poisons	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Nursing agencies licences	Licensing documentation regarding nursing agencies	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Other hazardous substances	Licensing documentation regarding other hazardous substances	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16

Licensing	Personal licences	Licensing documentation regarding fire safety and public entertainment	DESTROY – 2 years after registration lapses	Licensing Act 2003
Licensing	Pet shop licences	Licensing documentation regarding pet shops	DESTROY – 2 years after registration lapses	Pet Animals Act 1951 and 983
Licensing	Petroleum	Documentation regarding the licensing of petroleum	DESTROY – 2 years after registration lapses	Petroleum (Regulation) Act 1928 and 1936
Licensing	Premises licences	Documentation regarding premises licensing	DESTROY – 2 years after registration lapses	Licensing Act 2003
Licensing	Premises licences	Documentation regarding premises licensing	DESTROY – 2 years after registration lapses	Licensing Act 2003
Licensing	Premises licences	Documentation regarding entertainment licences	DESTROY – 2 years after registration lapses	Licensing Act 2003
Licensing	Private hire licences	Licensing documentation regarding private hire taxi services	DESTROY – 2 years after registration lapses	Local Government (Miscellaneous Provisions) Act 1976
Licensing	Public entertainment licences	Repealed by the Licensing Act 2003, retained for information already held	DESTROY – 2 years after registration lapses	Licensing Act 2003
Licensing	Riding establishment licences	Documentation regarding caravan and camp site licences	DESTROY – 2 years after registration lapses	Riding Establishments Act 1964 and 1970
Licensing	Sale of explosives licences	Documentation regarding the sale of explosives	DESTROY – 2 years after registration lapses	Manufacture and Storage of Explosives Regulations 2005
Licensing	Scrap Metal licences	Documentation regarding scrap metal licences	DESTROY – 2 years after registration lapses	Scrap Metal Dealers Act 1964
Licensing	Sex establishments	Documentation regarding sex establishment licences	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Shops	Documentation regarding the licensing of shops	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Scaffold licences	Documentation regarding scaffolding licences	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Skip Licences	Documentation regarding skip licences	DESTROY – 2 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Licensing	Street	Documentation regarding street	DESTROY – 2 years after	House to House Collections Act

	collections and lotteries licences	collection and lotteries licences	registration lapses	1939; Lotteries and Amusements Act 1976
Licensing	Street trading licences	Documentation regarding street trading licences	DESTROY – 2 years after registration lapses	Local Government (Miscellaneous Provisions) Act 1982
Licensing	Zoo licenses	Documentation regarding zoo licensing	DESTROY – 2 years after registration lapses	The Zoo Licensing Act 1981
Sex establishments		Consolidated list of licensed sex establishments	DESTROY – 3 years after registration lapses	Retention Guidelines for Local Authorities No. 9.16
Council Property				
Common Land				
Grazing		Information related to grazing on common land	DESTROY – 6 years from the creation of the agreement	Staffordshire County Council
Registration		The local authority is responsible for maintaining a register of common land and village greens within its boundaries	DESTROY – 10 years after creation	Countryside and Rights of Way Act 2000
Maintenance of Council Property				
Maintenance		Instruction manuals related to council property	DESTROY – 7 years after last action	Retention Guidelines for Local Authorities No. 7.27
Planned maintenance	Case files – Property	Documentation relating to the process of managing and undertaking planned maintenance of property	DESTROY – 7 years after last action	Retention Guidelines for Local Authorities No. 7.27
Refurbishment	Case files – Property	Documentation relating to the process of managing and undertaking planned renovations and development of property	DESTROY – 7 years after conclusion of transaction	Retention Guidelines for Local Authorities No. 8.7
Responsive maintenance	Case files - Property	Documentation relating to process of managing and undertaking emergency maintenance of property	DESTROY – 7 years after last action	Retention Guidelines for Local Authorities No. 7.27
Property Acquisition and Disposal				
Acquisitions	Case files - Property Assets over	Any papers concerning the management of the acquisition (by finance lease or purchase) process	DESTROY – 6 years after all obligations / entitlements concluded	Limitations Act 1980

	£5000	for real property council property.		
Acquisitions	Case files - Property Assets under £5000	Any papers concerning the management of the acquisition (by finance lease or purchase) process for real property council property.	DESTROY – 6 years after all obligations / entitlements concluded	Limitations Act 1980
Deeds	Case files - Property	Deeds and associated documentation	RETAIN – for life of property plus 12 years.	Limitations Act 1980
Disposal	Case files - Property	Documentation relating to the management of the disposal (by sale or by write off) process for real property	DESTROY – 12 years after all obligations / entitlements concluded	Limitations Act 1980
Disposal	Case files - Property	Documentation relating to the management of the disposal (by sale or by write off) process for real property	DESTROY – 6 years after all obligations / entitlements concluded	Limitations Act 1980
Disposal	Case files - Property	Information on the disposal of property	DESTROY – 15 years after all obligations / entitlements concluded	Retention Guidelines for Local Authorities No. 8.3
Property and Land Management				
Accessibility		Documentation and information relating to the access of property owned by the Council	DESTROY – 7 years from closure	Thurrock Council
Building surveys		Data collected from surveys conducted on council buildings	DESTROY – 2 years after date of issue	The National Archives Retention and Disposal Guidance 1.
Certification		Certificates of approval	REVIEW – 25 years after date of issue	The National Archives Retention and Disposal Guidance 1.
Distribution and allocation of properties		Documentation relating to the distribution of council property	DESTROY – 3 years from date of last action	Lancaster City Council
Energy management		Documentation concerned with energy management within the council's property	DESTROY – 5 years from date of last action	Eastbourne Borough Council
Energy management	Case files - Property	Papers concerning the management of energy within the council	DESTROY – 5 years from date of last action	Eastbourne Borough Council
Equipment		Process involved in the disposal of council equipment	DESTROY – once obsolete	Eastbourne Borough Council

Facilities management		Process involved in the management of council facilities	DESTROY – 10 years from date of last action	Lincolnshire County Council
Farm management		Documentation concerned with farm management	DESTROY – 1 year after document superseded	Staffordshire County Council
Feasibility		Process involved in checking the feasibility of council property	REVIEW – 25 years after the decision was taken	The National Archives Retention and Disposal Guidance 1.
Fleet management		Information on how vehicles have been allocated and maintained	DESTROY – 7 years after disposal of the vehicle	Retention Guidelines for Local Authorities No. 8.15
Fleet management		Information on drivers	DESTROY – 7 years after closure	Retention Guidelines for Local Authorities No. 8.17
Fleet management		Information on vehicle usage	DESTROY – 3 years after disposal of the vehicle	Retention Guidelines for Local Authorities No. 8.16
Fleet management		Documentation regarding the process of acquisition and disposal of vehicles through lease or purchase	DESTROY – 7 years after disposal of the vehicle	Retention Guidelines for Local Authorities No. 8.14
Health and safety	Case files - Property	Health and safety issues specific to property owned by the council	DESTROY – 1 year after process ceases or is superseded	Retention Guidelines for Local Authorities No. 9.6
Internal agreements	Case files - Property	Information and documentation specific to internal agreements concerning council property	DESTROY – 6 years after agreement ceases or is superseded	Limitation Act 1980
Land and property history	Case files - Property	Historical documents about council property and land owned by the council	DESTROY – 12 years from life of property	Retention Guidelines for Local Authorities No. 8.2
Leasing	Case files - Property	Documents relating to the process of managing leased property	DESTROY – 15 years after expiry of the lease	Retention Guidelines for Local Authorities No. 8.8
Leasing	Case files - Property	Documents relating to the process of managing the occupancy of the property	DESTROY – 7 years after conclusion	Retention Guidelines for Local Authorities No. 8.9
Management		The process of managing and undertaking renovations and development of property	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 8.5
Management		The process of managing and undertaking renovations and development of property	RETAIN for life of the building	Retention Guidelines for Local Authorities No. 8.6

Maps and directions	Case files - Property	Maps and directions relating to council property	REVIEW – 25 years after compilation	The National Archives Retention and Disposal Guidance 1.
Property services	Case files – Property	Documentation concerned with services provided from council property	DESTROY – 10 years from date of last action	Lincolnshire County Council
Property strategy		Overall reports on council property	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 8.1
Replacement programme		Documentation associated with replacement programmes	DESTROY – 12 years from last year	Dover District Council
Scheduling		Inventories of specific properties or assets contained within them.	DESTROY – 2 years from conclusion of admin use	Essex County Council
Security	Case files – Property	Documentation relating security and processes relating with security of the councils property	DESTROY – 1 month from date of creation	Staffordshire County Council
Usage statistics	Case files – Property	Any data held concerned with usage of council property	DESTROY – 2 years from conclusion of admin use	Essex County Council
Valuations	Case files – Property	Valuation documentation and statistics	DESTROY – 6 years from end of financial year after disposal of property	Thurrock Council
Property Use and Development				
Car parking	Case files – Property	Any documentation regarding the process of managing and undertaking renovations and development specific to car parking	DESTROY – 7 years after completion	Thurrock Council
Design and construction	Case files – Property	Documentation relating to the process of managing the design and construction of council property	DESTROY – 25 years after completion of works	The National Archives Retention and Disposal Guidance 1.
Traveller sites		Documentation relating to sites specifically designated as 'Traveller sites'	PERMANENT – 6 years from termination	Limitation Act 1980
Warehousing and storage		Process documentation concerning warehouse storage	DESTROY – 2 years from date of last action	Eastbourne Borough Council
Crematoria and Cemeteries				
Burial Identity and Location				
Registration		Documentation regarding the layout	DESTROY – 15 years after	Cremation (England and Wales)

		of the burial space in crematoria and cemeteries	creation	Regulations 2008 No. 2841
Registration		Includes: Burial register and plan of plot ownership and occupation. Crematorium Register of cremations and plan or ownership of interment of ashes	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 9.24
Bookings		Documentation related to booking made for a cremation, interment or monument erection	DESTROY – 5 years after last action	Retention Guidelines for Local Authorities No. 9.25
Exhumations		Documentation regarding the process of regulation of exhumation	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 9.24
Interment service		Process relating to the burial or cremation of an individual	DESTROY – 5 years after last action	Retention Guidelines for Local Authorities No. 9.25
Licensing		Documentation regarding cemetery and crematoria licensing	DESTROY – 5 years after last action	Retention Guidelines for Local Authorities No. 9.25
Memorial management		Records relating to the ordering of a memorial	DESTROY – once document superseded	Lancaster City Council
Maintenance of Burial Grounds				
Planned maintenance		Program of maintenance to cemeteries and crematoria over the next maintenance period	DESTROY – 21 years after maintenance completed	Thurrock Council
Redundant Churchyards		Documentation relating to discussed churchyards, specifically their upkeep	DESTROY – 21 years after maintenance completed	Thurrock Council
Responsive maintenance		Emergency or unplanned maintenance to cemeteries and crematoria	DESTROY – 21 years after maintenance completed	Thurrock Council
Democracy				
Decision Making				
Council and committee meetings		Agendas, meeting and minutes relating to full council decision making processes	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 1.4
Council and committee meetings		Agendas, meeting and minutes relating to full council decision making processes	DESTROY after date of confirmation of the minutes	Retention Guidelines for Local Authorities No. 1.5

Delegations		The process of delegating power to authorise an action and the seeking and granting permission to undertake a requested action	DESTROY – 6 years after delegation is superseded or ended	The National Archives Retention and Disposal Guidance 10.
Independent Remuneration Panel		Documentation relating to the Independent Remuneration Panel	DESTROY – 1 year from date of last action	Local Decision
Meeting – cabinet		Agendas, meeting and minutes relating to the executive board of members	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 1.4
Member panels		Agendas, meeting and minutes relating to member panels	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 1.4
Referenda		Management of democratic activities including elections, assembly and committee meetings	PERMANENT – Offer to Central Government	Lancaster City Council
Scrutiny panel		Agendas, meeting and minutes relating to the scrutiny panel	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 1.4
Executive				
Statutory Appointments		List of statutory appointments of the council	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 6.24
Statutory Appointments		The process of selection of an individual for a statutory position	DESTROY – 2 years after date of appointment	Retention Guidelines for Local Authorities No. 6.25
Governance				
Constitution		The constitution on the council	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 1.4
Honours and Awards				
Honours and submissions		The submissions and details of individuals considered for honours	DESTROY – 5 years after last action	Retention Guidelines for Local Authorities No. 1.8
Lord lieutenancy		Documentation relating to Lord Lieutenancy	DESTROY – 5 years from last action	Lancaster City Council
Member Support				
Gifts and hospitality		Register of gifts and hospitality	DESTROY – 18 months after member leaves office	Thurrock Council
Register of Interests		Members' disclosure of any involvement in organisations and income received from other bodies,	DESTROY – 18 months after member leaves office	Lancaster City Council

		which may affect their actions as council members		
Planning				
Cross departmental consideration		Reports and minutes	DESTROY – 3 years from closure	Retention Guidelines for Local Authorities No. 2.3
Forward plan		The list of items to be considered by the cabinet over the next four months	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 2.1
Strategic plan		Strategic management team minutes	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 2.2
Strategic plan		Monitoring and reviewing strategic plans	Destroy – 5 years from closure	Retention Guidelines for Local Authorities No. 2.7
Representation				
Constituencies	Meetings regarding constituencies	Ward names, numbers and boundaries	DESTROY – 6 years from date of meeting	Local Decision
Elections		The activities carried out in the process of electing representatives at parish, district, county, parliamentary and European constituency level	DESTROY – 6 months from close of poll	Records Management Society of Great Britain
Elections		European election ballot papers	DESTROY – 1 year after elections	European Parliamentary Elections Regulations 1999
Elections		Local election ballot papers	DESTROY – 6 months from close of poll	Representation of the People Regulations 1986; Local Elections (Parishes and Communities) Rules 1986
Elections		Election results	DESTROY – 6 months from close of poll	Retention Guidelines for Local Authorities No. 1.3
Elections		Summary certification of those eligible to vote	PERMANENT – offer to archivist	Representation of the People Regulations 1986
Elections		The list of people registered to vote	DESTROY – 6 months from close of poll	Records Management Society of Great Britain
Emparishment		The process in creating a new civil parish council	PERMANENT – offer to archivist	Local Decision
Lists of councillors		Public contact details of your local	PERMANENT – offer to	Access to Information Act 1985

		representative of the council	archivist	
Lists of meetings		List of meetings of Council and committees	PERMANENT – offer to archivist	Lancaster City Council
Nominations		Listing of members and others representing the council on external bodies. Official delegation to represent council's interests. Includes membership of other bodies	DESTROY – 5 years from date of last action	Lancaster City Council
Political parties' papers		Leader of council papers, leader of opposition papers	DESTROY – 3 years after last action	Retention Guidelines for Local Authorities No. 1.9
Economic Development				
Business Intelligence				
Business listing		Listing of businesses trading within the local area. Only organisations that have requested inclusion included	PERMANENT – offer to archivist	Staffordshire County Council
European development		Information collected regarding European funding	DESTROY – once record become obsolete / no longer required	Staffordshire County Council
Marketing		The collection and management of the economic and social data about the local area	DESTROY – 20 years after collected New census info only arrives every 10 years and updated indices of deprivation data every 4 – 5 years. Need to retain to analyse time series	Thurrock Council
Promotion				
Advice to business		Information on providing advice to new or existing businesses	DESTROY – 6 years from date of creation	Staffordshire County Council
Business awards		Information regarding business awards and grants	DESTROY – 7 years after scheme to which grant relates is completed	Thurrock Council
Business development		Information about activities designed to develop and encourage business development in the local area.	DESTROY – 2 years from date created	Staffordshire County Council

		Including externally funded projects and sustainability		
Business development		Information about activities designed to develop and encourage business development in the local area. Including externally funded projects and sustainability	DESTROY – 2 years from date created	Staffordshire County Council
Film and television development		To promote the area as a location and centre of excellence for the film and broadcasting industries	DESTROY – After 7 years	Eastbourne Borough Council
International relations		Encouraging relations with people from other countries and cultures to support the development of the local area	PERMANENT – offer to archivist	Staffordshire County Council
List of properties		A list of properties or land currently available to let within the area	DESTROY – 6 years from date of creation	Staffordshire County Council
Markets		Information about markets including farmers markets	DESTROY – 6 years from date of creation	Limitation Act 1980
Voluntary sector development		The information relating to the encouragement of the voluntary sector activity	PERMANENT – offer to archivist	Staffordshire County Council
Regeneration				
Community development		Information relating to revitalising a specific area or community	DESTROY – 10 years from end of the project	Eastbourne Borough Council
Regional development		Participation in regional activities	DESTROY – 10 years from end of the project	Eastbourne Borough Council
Rural development		Information relating to reducing disadvantage and increasing access in rural areas	DESTROY – 6 years from date plan superseded	Eastbourne Borough Council
Strategy		Information relating to revitalising a specific area or community	PERMANENT – Offer to archivist when plan superseded	Eastbourne Borough Council
Town centre management		Information relating to the management of business community in the town centres	PERMANENT – Offer to archivist when plan superseded	Eastbourne Borough Council

Sustainability				
Sustainable development		Information and documentation looking at sustainable development	REVIEW – paper file 9 years from date of creation DESTROY – electronic file 7 years from closure of paper file	Staffordshire County Council
Tourism				
Tourism development		The information relating to the development of tourism	DESTROY – after 6 years	Staffordshire County Council
Training				
Workforce support		Information about activities to support continued employment in the area	DESTROY – 1 year from date of creation	Records Management Society of Great Britain
Education and Skills				
Access and Inclusion				
Project management		Educational access and inclusion related projects	DESTROY – 10 years from date of project completion	The National Archives Retention and Disposal Guidance 6.
Traveller sites		Activities aimed at ensuring access to education for travellers	DESTROY – 7 years after closure of project	Thurrock Council
Admissions and Exclusions				
Appeals		The process to question a decision or allocation which has been given	DESTROY – 7 years after decision is made	Thurrock Council
Parental choice		General information involved regarding choosing a school	DESTROY – 7 years after application is made	Local Decision
Parental choice		Information specifically concerning school directories	DESTROY – 7 years after last action	Local Decision
Advice				
Advisory services		Documentation on the different advisory services provided regarding education and skills	DESTROY – 6 years from last action	Staffordshire County Council
Arts Services				
Field centres		Utilisation and management of field centres in arts education	DESTROY – after 7 years	Thurrock Council
Music services		Music tuition provided for individuals or groups within schools or music	DESTROY – after 7 years	Thurrock Council

		centres		
Provision in schools	Orders and bookings	Organisation and management of bookings for arts performances	DESTROY – after 7 years	Thurrock Council
Performances		Orders and bookings made for arts services made by schools	DESTROY – after 7 years	Thurrock Council
Curriculum Development				
International projects		Information on international projects	DESTROY – 10 years after project completion	The National Archives Retention and Disposal Guidance 6.
National curriculum		Helping schools and teachers develop the curriculum within schools	DESTROY – after 7 years	Thurrock Council
Out of schools projects		Data and information on out of school projects i.e. after school clubs, outings etc…	DESTROY – after 7 years	Thurrock Council
Outdoor education		Documentation on the countryside with regards to outdoor education	DESTROY – 6 years from date document superseded	Staffordshire County Council
Schools curricula		Helping schools and teachers develop the curriculum within schools	DESTROY – after 7 years	Thurrock Council
Education Welfare				
Attendance and Truancy		Data collected by student services on behaviour and attendance	DESTROY – 3 years after date of last entry	The Education (Pupil Registration) Regulations 1995 No. 2089
Student welfare service		Documentation regarding student service and the support they provide	DESTROY – 6 years from last action	Staffordshire County Council
Employment Skills				
Careers advice		The provision of careers advice	DESTROY – 6 years from end of current school year	Staffordshire County Council
Workplace training		The process of developing the workforce skill	DESTROY – 6 years from date document superseded	Staffordshire County Council
Life Long Learning				
Adult and community services		Learning for all ages including non school, college or university settings	DESTROY – 5 years from date of last action	Lincolnshire County Council
Basic skills development		Process to develop a basic level of skills and competencies	DESTROY – 5 years from date of last action	Lincolnshire County Council
Basic skills development	Course directory	Information on the different courses available to adults	DESTROY – 5 years from date of last action	Lincolnshire County Council

Management of Schools				
Admissions	School files	The process of admitting students to schools	DESTROY – 3 years after date of entry	The Education (Pupil Registration) Regulations 1995 No. 2089
Emergency contacts	School files	Details of emergency contacts	RETAIN – until information superseded	Lincolnshire County Council
General information	School files	General information involved regarding the school's holiday etc...	RETAIN – until information superseded	Lincolnshire County Council
Governing bodies	School files	A school is governed by a body like the board of a limited company – information, service and assistance for school governors	PERMANENT – offer to archivist	Staffordshire County Council
Governing bodies	School files	Minutes of the school governors	DESTROY – 3 years after the event	Staffordshire County Council
Governor contacts	School files	Contact details of the school governors	DESTROY – 5 years after governor leaves	Thurrock Council
Health and nursing	School files	School nursing and health promotion	DESTROY – 2 years from date of leaving school	Staffordshire County Council
Inspections	School files	Details on inspections carried out within a school, specifically about dangerous structures	DESTROY – 6 years from date of inspection	Staffordshire County Council
Performance	School files	The results an individual school has achieved, classified by school Key Stage 2 SATs results for primary schools and GCSE / A level results for secondary schools	REVIEW - every 7 years and then offer to archivist	Thurrock Council
Plans and policies	School files	Plans and policies developed by the schools	RETAIN – while policy is operational then offer to archivist	Thurrock Council
School catering	School files	School meals and nutritional information	DESTROY – 3 years after last action	Lincolnshire County Council
Teaching				
Mentoring		The provision of learning mentors	DESTROY – 2 years from last action	Lincolnshire County Council
Teacher development		Activities relating to the provision and	DESTROY – 7 years from	Lincolnshire County Council

		support for education and learning	last action	
Environmental Protection				
Advice				
Biodiversity		Information regarding biodiversity	PERMANENT – offer to archivist after administrative use completed	Thurrock Council
Campaigns		Documentation regarding campaigns specifically concerning environmental protection	PERMANENT – offer to archivist after administrative use completed	Thurrock Council
Conservation				
Archaeological services		Provision of archaeological services and consultation to both commercial and public sector clients in the local area	DESTROY – After 5 years unless still live	Lincolnshire County Council
Countryside conservation		Documentation relating to the management of the countryside	PERMANENT – offer to archivist after administrative use completed	Thurrock Council
Forest management		Documentation relating to the management of forests	PERMANENT – offer to archivist after administrative use completed	Thurrock Council
Heritage conservation		Documentation looking specifically at heritage conservation	PERMANENT – offer to archivist after administrative use completed	Thurrock Council
Nature conservation		Documentation looking specifically at nature conservation	PERMANENT – offer to archivist after administrative use completed	Thurrock Council
Urban conservation		Documentation relating to conservation on towns and cities	PERMANENT – offer to archivist after administrative use completed	Thurrock Council
Woodland management		Documentation relating to the management of woodland	PERMANENT – offer to archivist after administrative use completed	Thurrock Council
Monitoring				
Coastal erosion		Data and information on coastal erosion	PERMANENT – offer to archivist after administrative	Thurrock Council

			use completed	
Environmental impact assessment		Documentation relating to environmental impact assessments	PERMANENT – offer to archivist after administrative use completed	Thurrock Council
Environmentally sensitive areas		Data held concerning environmentally sensitive areas	PERMANENT – offer to archivist after administrative use completed	Thurrock Council
Finance				
Accounts and Audit				
Internal auditing		Activities relating to internal or external auditing of the authority	DESTROY – 6 years after current year	Accounts and Audit Regulations 2003 No. 533
Reporting		Activities relating to the consolidation of financial transactions and the production of financial statements. Includes ledges, monthly management accounts and statutory returns	DESTROY – 6 years after current year	Local Government Act 2003; VAT Act 1994; Taxes Management Act 1970; Audit Commission Act 1998
Reporting		Accounting reports	DESTROY – 6 years after current year	Local Government Act 2003
Asset Management				
Maintaining assets		Activities relating to collection of information about the authority's fixed assets for accounting purposes	DESTROY – 6 years after asset is disposed of	The National Archives Retention and Disposal Guidance 10.
Maintaining assets		Information on plant and equipment	DESTROY – 7 years after sale or disposal of asset	Retention Guidelines for Local Authorities No. 7.27
Maintaining assets		Information on maintenance of other assets	DESTROY – 7 years after last action	Retention Guidelines for Local Authorities No. 7.28
Maintaining assets		Overall list of assets	DESTROY – 6 years after current year	Accounts and Audit Regulations 2003 No. 533
Maintaining assets		Reports and review of assets	DESTROY – 6 years after current year	Accounts and Audit Regulations 2003 No. 533
Maintaining assets		Summary reports on assets	DESTROY – 7 years after transaction was concluded	Retention Guidelines for Local Authorities No. 7.25

Financial Provision Management				
Borrowing		Activities relating to the borrowing of money by the authority. Includes mortgages	DESTROY – 7 years after the loan has been repaid	Retention Guidelines for Local Authorities No. 7.14
Borrowing		Summary management of loans	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 7.15
Budget		Activities involved in planning and monitoring the authority's annual budget. Includes allocation of budget to administrative units within the authority. For longer term planning, see Strategy and planning.	DESTROY – 6 years after current year	Local Government Act 2003
Budget		Information relating to the development of the budget	DESTROY – 2 years after budget adopted	Retention Guidelines for Local Authorities No. 7.12
Budget		Actual against planned revenue and expenses	DESTROY – after next years budget has been adopted	Retention Guidelines for Local Authorities No. 7.13
Debt management	Records relating to unrecoverable revenue, debts and overpayments - including register of debts written off, register of refunds, etc	Activities involved in managing debts owed to the council	DESTROY – 7 years from date of last action	Gedling Borough Council
Donations		Activities involved in the administration of donation to the authority. For administration of grant funding, see funding bids	DESTROY – 5 years from date of receipt	Eastbourne Borough Council
Funding bids		Activities relating to the applications by the authority for grant funding by	DESTROY – 6 years after action completion/grant	The National Archives Retention and Disposal Guidance 10.

		external bodies. For applications to the authority for funding, see Funding applications	made	
Strategy and planning		Activities involved in the long term planning of the authority's financial management. Includes the financial forecast. For annual budget planning, see Budget	DESTROY – 6 years from end of planning cycle to which document relates	Eastbourne Borough Council
Financial Transactions Management				
Authorisation		Activities involved in delegating authority for carrying out financial activities on behalf of the authority	DESTROY – 6 years after conclusion of the financial transaction the record supports	Eastbourne Borough Council
Expenditure		Activities involved in the payment for goods and services by the authority. Includes expenses claims and honorariums. For records relating to benefit claims, see benefits and subsidies	DESTROY – 6 years after the conclusion of the transaction	Limitations Act 1980; VAT Act 1994; Taxes Management Act 1970; Audit Commission Act 1998
Expenditure		Travel expenses	DESTROY – 6 years after the conclusion of the transaction	Limitations Act 1980; VAT Act 1994; Taxes Management Act 1970; Audit Commission Act 1998
Fraud		Activities relating to the detection, prevention and prosecution of financial irregularity	**Fraud Investigations:** Keep for 2 years before considering disposal. **Fraud Prosecutions:** Keep for 6 years before considering disposal.	Local Decision based on Data Protection Act (1998) Principle 5
Funding application		Activities relating to the process of considering and administering applications to the authority for grant funding. For application by the authority for grant funding, see Funding bids	DESTROY – 6 years after conclusion of financial transaction the record supports	Eastbourne Borough Council
Income		Activities involved in the collection of	DESTROY – 6 years after	Eastbourne Borough Council

		money owed to the council. Includes rent payments	conclusion of financial transaction the record supports	
Internal recharging		The mechanism for recharging costs within the council	DESTROY – 6 years after conclusion of financial transaction the record supports	Eastbourne Borough Council
Investments		Activities relating to the investment of the authority's funds	DESTROY – 2 years after investments are liquidated/matured	Eastbourne Borough Council
National insurance numbers		Processes involved in the collection of National Insurance Numbers	DESTROY – 2 years after the employee ceases employment	Retention Guidelines for Local Authorities No. 7.8
Reconciliation		Activities involved in the reconciliation of accounts	DESTROY – 2 years after administrative use is concluded	Retention Guidelines for Local Authorities No. 7.6
Refunds		Documentation relating to refunds	DESTROY – 6 years after transaction	The National Archives Retention and Disposal Guidance 3.
Local Taxation				
Benefits and subsidies		Activities involved in the administration of benefits payments	DESTROY – 5 years after end of financial year	Records Management society of Great Britain
Business rates		Business rates information (other than property valuation)	DESTROY – 5 years after end of financial year	Records Management society of Great Britain
Council tax		Council tax information	DESTROY – 5 years after end of financial year	Taxes Management Act 1970
Property valuation		Valuation of assets other than property	DESTROY – 10 years after valuation was made	Retention Guidelines for Local Authorities No. 7.20
Property valuation		Rateable property information	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 7.21
Property valuation		Documentation relating to property valuation	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 7.20
National Taxation				
Tax payments		Activities involved in managing the payment of taxes by the authority	DESTROY – 7 years after last action	Retention Guidelines for Local Authorities No. 7.22
Tax payments		Activities involved in managing the	DESTROY – 5 years after	Limitation Act 1980; VAT Act 1994;

		payment of taxes by the authority	the end of the financial year	Taxes Management Act 1970; Audit Commission Act 1998
Payroll and Pensions				
Pay		Activities involved in the administration of remuneration to staff of the authority	DESTROY – 7 years after the conclusion of the transaction	Taxes Management Act 1970; Audit Commission Act 1998.
Pay		Non accountable processes relating to payment of employees	DESTROY – After administrative use is concluded	Retention Guidelines for Local Authorities No. 7.10
Pensions		Activities involved in the administration of pension schemes for current and former employees	DESTROY – 6 years after end of financial year	The Registered Pension Schemes (Provision of Information) Regulations 2006 No. 567
Health and Safety				
Community Safety				
Campaigns		Campaigns to promote compliance to health and safety policies	PERMANENT – offer to archivist	Eastbourne Borough Council
Compliance				
Strategy and planning		Establishment of a strong health and safety work culture in order the ensure compliance with health and safety legislation and provide a safe and healthy working environment for employees	DESTROY – 1 year after process ceases or is superseded	Retention Guidelines for Local Authorities No. 9.6
Strategy and planning		Health and safety policies	DESTROY – 6 years from last amendment	Health and Safety at Work Act 1974
Training		Documentation relating to health and safety training	DESTROY – 50 years after training is completed	Gedling Borough Council
Monitoring				
Accidents and incident reporting		Information about the reporting of individual accidents and actions resulting from them	DESTROY – 3 years after current year	Reporting of Injuries Diseases and Dangerous Occurrences Regulations 1995
Accidents and incidents reporting	Accident books – records	Registers of accidents and incidents	DESTROY – 3 years after current year	Reporting of Injuries Diseases and Dangerous Occurrences Regulations 1995
Accidents and incidents	Accident	Registers of accidents and incidents	DESTROY – 3 years after	Reporting of Injuries Diseases and

reporting	books – children		current year	Dangerous Occurrences Regulations 1995
Asbestos inspections		Monitor the condition of known asbestos products within building	DESTROY – 50 years from last action or age 75 years from date of birth (whichever is greater)	Control of Asbestos at Work Regulations 1987
Equipment		Process of inspecting equipment to ensure it is safe	DESTROY – 10 years after date of inspection	The National Archives Retention and Disposal Guidance 4.
Hazardous substances		Control and monitor the use of hazardous substances at work	DESTROY – 5 years from termination	The Control of Substances Hazardous to Health Regulations 2002 (amends 1989 Act)
Health and safety inspections		Activities relating to internal or external inspections examining the authority's health and safety provision	DESTROY – 5 years from termination	The Control of Substances Hazardous to Health Regulations 2002 (amends 1989 Act)
Radiation		Monitoring of radiation	DESTROY – 40 years from last action	The Ionising Radiations Regulations 1985
Risk Management				
Risk assessments		Activities relating to the risk assessments carried out by the authority. Includes workplace assessments	DESTROY – 3 years after last assessment	Management of Health and Safety at Work Regulations 1992
Housing				
Advice				
Advice to homeowners and tenants		Help and advice to private tenants or landlords	DESTROY – 2 Years from last action	Dover District Council
Enforcement				
Assessment – housing standards		Assessment of housing standards	DESTROY – 2 Years from last action	Wychavon District Council
Safety inspections		Safety inspection on homes in multiple occupation	DESTROY – 2 Years from last action	Wychavon District Council
Estate Management				
Business premises		Documentation relating to the inspections and monitoring of the environment of business premises	DESTROY – 7 years from last action	Records Management Society
Car parking surveys		Documentation relating to the	DESTROY – Once	Eastbourne Borough Council

		inspections and monitoring of the environment of council estate car parks	superseded	
Garage application		Application for garage space	Unsuccessful – DESTROY – 6 month from closure of file Successful – DESTROY – 1 year from termination of contract	Lancaster City Council
Garage rental	Tenant file	Documentation relating to garage rental and allocation	DESTROY – 1 year from termination of contract	Lancaster City Council
Housing inspections		Documentation relating to the inspection and monitoring of the environment of the council housing estate	DESTROY – 2 years from last action	Wychavon District Council
Neighbourhood disputes		Documentation relating to the resolution of neighbour disputes involving council tenants	DESTROY – 5 years from resolution of dispute	Liverpool City Council
Housing Provision				
Allocations		Information relating to the process of allocating property (homes and garages) to applicants on the waiting list.	DESTROY – 2 years from last action	Wychavon District Council
Assessment – housing needs		Assessment of whether applicant is eligible for service or judgement about what service we should provide	DESTROY – 6 years from last action	Wychavon District Council
Homelessness		Process in providing short term and emergency accommodations for homeless people	DESTROY – 3 years from closure of record	Lancaster City Council
Hostel providers		Documentation relating to hostel providers an youth hostels in general	DESTROY – 7 years from last action	Lancaster City Council
Housing applications		Documents related to housing applications	DESTROY – 7 years from closure	Retention Guidelines for Local Authorities No. 3.27
Housing applications	Unsuccessful applications	Documents related to unsuccessful housing applications	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 3.26
Housing applications	Council	The register of individual housing	PERMANENT – offer to	Lancaster City Council

	housing register	applications	archivist	
Housing exchange	Mutual exchange list	Current register of properties available for exchange	DESTROY – 4 years from last action	Retention Guidelines for Local Authorities No. 8.10
Housing stock requirements		Information on amount and type of housing stock required	DESTROY – 3 years from end of financial year to which the record relates	Lancaster City Council
Landlord accreditation		Landlord accreditation schemes	DESTROY – 5 years from date of expiry	Chichester and Arun District Council
Sheltered housing		Information on the provision of sheltered housing	DESTROY – 7 years from last action	Lancaster City Council
Housing Stock				
Demolition	Property file	Demolition of housing stock	PERMANENT – offer to archivist	Dover District Council
Emergency maintenance	Property file	Emergency or unplanned maintenance to council housing	DESTROY – 6 years from date of last action	Wychavon District Council
Housing grants	Property file - Grants of £ 50,000	Documentation relating to housing grants	DESTROY – 12 years after last payment	Limitations Act 1980
Housing grants	Property file - Grants under £50,000	Documentation relating to housing grants	DESTROY – 6 years after last payment	Limitations Act 1980
Leases	Property file	Documentation relating to housing deeds	DESTROY – 6 years from date of expiry	Limitations Act 1980
Planned maintenance	Property file	Program of maintenance to council housing over the next maintenance period	DESTROY – 7 years from last action	Nottingham City Council
Private housing grants	Property file	Provision of grant assistance to improve the condition of private housing	DESTROY – 12 years from last payment for grants over £50k DESTROY – 6 years from last payment for grants under £50k	Nottingham City Council
Property adaptations	Property file	Details of properties adapted to clients' needs	DESTROY – 6 years from last action	Essex County Council

Repairs and renovation	Property file	Documents relating to repairs and renovation of housing	DESTROY – 7 years from last action for repairs RETAIN – information relating to renovations for the life of the property	Essex County Council
Risk assessment	Asbestos register	Register of asbestos in council housing	DESTROY – 50 years from last action or 75 years from date of birth (whichever is greater)	Control of asbestos at work regulations 1987
Unauthorised occupants		Squatters and unauthorised occupants	DESTROY – 7 years from last action	Records Management Society of Great Britain
Managing Tenancies				
Adaptations	Property file	Discretionary assistance to disabled and elderly council tenants for their dwellings and gardens outside of normal tenancy arrangement	DESTROY – 16 years from expiry or termination of lease	The National Archives Retention and Disposal Guidance 1.
Adaptations grants	Property file	Provision of grant assistance to the adapting of homes	DESTROY – 6 years from last action	Limitation Act 1980
Advice	Tenant file	Advice given to council tenants	DESTROY – 2 years from end of year record was created	Dover District Council
Agreements	Tenant file - Ordinary tenancy	Documentation relating to the tenancy agreement	DESTROY – 6 years after tenancy has expired	Limitations Act 1980
Agreements	Tenant file - Tenancy under seal	Documentation relating to the tenancy agreement	DESTROY – 12 years after tenancy has expired	Limitations Act 1980
Approving alterations	Property file	Permission requested by tenants to undertake alterations	DESTROY – 6 years from last action	Dover District Council
Assessment – housing needs	Tenant file	Assessment whether application is eligible for services or judgement about what service we should provide	DESTROY – 6 years from last action	Wychavon District Council
Breaches	Tenant file	Documentation relating to the notification and enforcement of breaches of council tenancy	DESTROY – 12 years from termination of tenancy	Lancaster City Council

		agreements. Includes rent arrears.		
Evictions	Tenant file	Documentation relating to evictions of specific tenants	PERMANENT – offer to archivist	Dover District Council
Housing repairs	Tenant file	Housing repairs documentation relating to specific properties	DESTROY – 7 years from last action	Wychavon District Council
Insurance		Contents insurance for council tenants	DESTROY – 7 years from policy expiration	Sefton Council
Rent arrears	Tenant file	Documentation relating to the notification and enforcement of breaches of council tenancy agreements. Includes rent arrears	DESTROY – 6 years from last action	Limitation Act 1980
Rent setting		Documentation relating to rent setting of housing	DESTROY – 7 years from end of financial year the record was created in	Sefton Council
Right to buy	Tenant file	Documentation relating to tenants statutory right to purchase council housing	DESTROY – 12 years after sale of house	Limitation Act 1980
Temporary accommodation	Tenant file	Provision of temporary accommodation	DESTROY – 7 years from last action	Lancaster City Council
Tenancies	Tenant file	Personal details relating to tenancies held	DESTROY – 6 years from last action	Lancaster City Council
Welfare services	Tenant file	Services associated with disadvantaged persons to enable them to continue living in their home/community	DESTROY – 3 years from date of last action	Lancaster City Council
Human Resources				
Administering Employees				
Counselling	Employee files	Documentation relating to counselling offered to an employee	DESTROY – 6 years from termination of employment	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Absence monitoring	Employee files	Records documenting an employee's absence due to sickness	DESTROY – 6 years after termination of employment	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Discipline	Employee files	Documentation relating to the discipline of employees	DESTROY – 6 years after termination of employment	Employment Practices Data Protection Code Part 1: Recruitment

				and Selection 2002
Discipline	Employee files	Disciplinary warnings – final	DESTROY – 6 years after termination of employment	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Discipline	Employee files	Proceedings where it is proven to be unfounded	DESTROY – 6 years after termination of employment	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Discipline	Employee files	Disciplinary warnings - oral	DESTROY – 6 years after termination of employment	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Discipline	Employee files	Disciplinary warnings – behaviour to children	DESTROY – 6 years after termination of employment	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Discipline	Employee files	Disciplinary warnings – written	DESTROY – 6 years after termination of employment	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Disclosure of interest		Register of declared interests of employees in relation to anything being transacted or discussed b the authority	DESTROY – 6 years from termination of employment	Local Decision
Employee details	Employee files	Documentation relating to individuals general or specific condition of employment	DESTROY – 6 years from termination of employment	Thurrock Council
Employment conditions	Employee files	Documentation relating to individuals general or specific conditions of employment	DESTROY – 100 years after employment ceases	The National Archives Retention and Disposal Guidance 2.
Grievances	Employee files	Documentation relating to grievances between the employer and employee's	DESTROY – 6 years from termination of employment	Thurrock Council
Individual training records	Employee files	Documentation relating to an individuals training record and any work experience undertaken within the authority	DESTROY – 6 years from termination of employment	Thurrock Council
Individual training records	Employee files	Documentation relating to proof of training course completion	DESTROY – 7 years after course completed	Thurrock Council

Induction		Documentation relating to the process and undertaking of induction for new employees or councillors	DESTROY – 2 years after closure	Thurrock Council
Job evaluation		Documentation relating to the approach to performance appraisals	DESTROY – 6 years from termination	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Leave	Employee files	Documentation relating to the requested employee leave: annual, study, carers, special, compassionate, unpaid leave etc...	DESTROY – 2 years after action is completed	Retention Guidelines for Local Authorities No. 6.13
Medical assessments	Employee files	Documentation regarding medical assessments and general information on healthy living	DESTROY – 75 years from date of birth	Retention Guidelines for Local Authorities No. 6.10
Maternity / Paternity	Employee files	Records documenting entitlements to and calculations of, Statutory Maternity Pay.	DESTROY – 3 years from end of current tax year	Thurrock Council
Reporting		Reports related to working hours and terms and conditions	DESTROY – 6 years from termination of employment	Local Decision
Termination		Documentation relating to the leaving process: resignation, termination other than pensions.	DESTROY – 6 years from termination of employment	Retention Guidelines for Local Authorities No. 6.16
Employee Relations				
Disciplinary matters reporting		Summary management information relating to disciplinary matters	RETAIN – on personal file until normal file disposal. Warnings involving children/vulnerable adults retained for 25 years after end of employment	Records Management Society of Great Britain
Trade union liaison		Matters relating to the relationship with recognised unions	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 6.5
Trade union liaison		Documentation relating to liaison with unions and employee representative organisations	DESTROY – 2 years after use is concluded	Retention Guidelines for Local Authorities No. 6.6
Equal Opportunities				
Equalities and diversity		Equality and diversity documents	DESTROY – 5 years after	Records Management Society of

		which include information on fair treatment of employees and general guidelines	action completed	Great Britain
Equalities and diversity		Investigation and reporting on specific cases	DESTROY – 5 years after action completed	Retention Guidelines for Local Authorities No. 6.9
Monitoring Employees				
Performance appraisal		Documentation relating to the performance appraisal of an employee, including performance related pay if applicable	DESTROY – 5 years after action completed	Records Management Society of Great Britain
Reporting		Staff statistic documentation	DESTROY – 5 years after action is completed	Retention Guidelines for Local Authorities No. 6.12
Staff directory		Employee / sectional contact details	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 6.1
Occupational Health				
Absence reporting		Aggregated management information on absences, for instance, working days lost to various sickness categories	DESTROY – 3 years after the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982; Statutory Maternity Pay and Statutory Sick Pay (Miscellaneous Amendments) Regulations 2002
Occupational health		Documentation relating to occupational health and safety	DESTROY – 75 years after date of birth	Retention Guidelines for Local Authorities No. 6.10
Occupational health	Employee files	Occupational health and safety training	DESTROY – 50 years after training completed	Retention Guidelines for Local Authorities No. 6.19
Personal risk assessments	Employee files	Including restrictions i.e. cannot lift or desk work only	DESTROY – 6 years after termination of employment	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Sickness monitoring	Employee files	Documentation relating to sickness absence, including medical certificates	DESTROY – 6 years after termination of employment	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Major injuries		Documentation elating to major injuries	DESTROY – 40 years after termination of employment	Health and Safety at Work Act 1974; Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 reg. 7
Recruitment				

Authorisation		Authorisation to recruit for a position	DESTROY – 6 years after termination	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Job descriptions		The job descriptions and person specifications for current posts	DESTROY – 6 years after termination	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Recruitment		Process relating to the recruitment of an employee to the authority	DESTROY – 6 years from termination of employment	Retention Guidelines for Local Authorities No. 6.4
Recruitment	Position	Documents relating to unsuccessful candidates	DESTROY – 6 months after recruitment finalised	Thurrock Council
Recruitment	Position	Selection for a position	DESTROY – 1 year after recruitment finalised	Retention Guidelines for Local Authorities No. 6.11
Recruitment process		Documentation relating to the recruitment process	DESTROY – 1 year after recruitment finalised	Records Management Society of Great Britain
Secondment	Secondment files	Documentation relating t the process of secondments to or from the authority	DESTROY – 6 years after termination of employment	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Volunteers	Volunteer files	Documentation relating to volunteers available to or used by the council, including risk assessments	DESTROY – 6 years after termination of employment	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Terms and Conditions of Employment				
Staff benefits		Documentation relating to staff benefits	DESTROY – 6 years after termination of employment	Records Management Society of Great Britain
Staff facilities		Documentation regarding facilities for staff including proposals for leisure facilities and eateries	DESTROY – 6 years after action completed	Local Decision
Staff recognition		Staff recognition documentation	DESTROY - 7 years after termination of employment.	Records Management Society of Great Britain
Terms and conditions		The general terms and conditions of employment with the council	DESTROY - 6 years after termination of employment. Some groups of employees are kept for 25 years after leaving date, i.e. employees for whom a CRB disclosure has been obtained	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002

			and leavers where there have been known concerns about their behaviour/conduct in relation to children or vulnerable adults	
Training				
Driver training		Driver training documentation	DESTROY – 6 years after termination	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Reporting		Performance management relating to training and development, including feedback statistics	DESTROY – 6 years after termination	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Support training		Training provided to support individuals or organisations working with of for clients	DESTROY – 6 years after termination	Employment Practices Data Protection Code Part 1: Recruitment and Selection 2002
Training courses	Training course files	Training documentation relating to specific courses and sessions	DESTROY – 2 years after action completed	Retention Guidelines for Local Authorities No. 6.17
Training courses	Training course files	Training courses concerning children	DESTROY – 35 years after courses completed, or last entry	Retention Guidelines for Local Authorities No. 6.18
Training courses	Training course files	Training course materials	DESTROY – 1 year after course superseded	Retention Guidelines for Local Authorities No. 6.20
Training courses	Training course files	Documentation relating to training courses and initiatives	DESTROY – 2 years after action superseded	Retention Guidelines for Local Authorities No. 6.17
Training plan	Training course files	Listing of corporate training activities and forward plans. Includes health and safety training	DESTROY – 6 years after training completion	Records Management Society of Great Britain
Workforce Planning				
Workforce development planning		Documentation relating to workforce management	DESTROY – 7 years after action completed	Retention Guidelines for Local Authorities No. 6.15
Workforce development planning		Documentation relating to workforce management and salaries	DESTROY – 3 years after action completed	Retention Guidelines for Local Authorities No. 6.14
Information and Communication Technology				
Infrastructure				

Disposal		Documentation relating to the process of disposal of hardware and software belonging to this authority	DESTROY – 6 years after all obligations / entitlements concluded	Retention Guidelines for Local Authorities No. 7.29
Disposal		Documentation relating to the process of disposal of hardware and software belonging to this authority	DESTROY – 12 years after all obligations / entitlements concluded	Retention Guidelines for Local Authorities No. 7.29
Fault reporting		Customer (Public) reporting of faults relating to council services	DESTROY – at end of operational life	Kent County Council
Licensing		Documentation in relation to software licensing	DESTROY – 6 years from termination	Limitation Act 1980
Help Desk support		Help desk support information relating to specific system or pieces of software	DESTROY – 2 years from date of last action	Local Decision
Information security		Data security information and documentation	REVIEW – 5 years from date of creation	The National Archives Retention and Disposal Guidance 9.
Network maintenance		Documentation relating to the maintenance and support of the network	RETAIN – Until end of systems life	Eastbourne Borough Council
Server maintenance		Documentation relating to system servers and their maintenance	RETAIN – Until end of systems life	Eastbourne Borough Council
Spatial data management		Documentation relating to geographical information systems	DESTROY – at the end of system life	Local Decision
Storage	Server Storage records	Documentation relating to storage systems and servers	RETAIN – Until end of systems life	Eastbourne Borough Council
Strategy	ICT Strategy	Documentation relating to an ICT strategy	DESTROY – once operational use is complete	Kent County Council
Web development		Includes development of Internet, Intranet and Extranet	DESTROY – 3 years from date of last action	Kent County Council
System Support				
Change control	System log	Documentation relating to planned changes to a specific system	DESTROY – 2 years after system no longer in use	Thurrock Council
Configuration management	System log	Documentations relating to the configuration of the system	DESTROY – 2 years after system no longer in use	Thurrock Council
Data management	System log	Documentation relating to the	DESTROY – 2 years after	Thurrock Council

		management of specific systems data which includes backups, mirroring and system interfaces	system no longer in use	
Design and construction	System log	Documentation relating to the design and construction of systems	DESTROY – 2 years after system no longer in use	Thurrock Council
Development	System log	Documentation relating to the development of systems and software. Includes web technology development, programming.	DESTROY – 2 years after system no longer in use	Thurrock Council
Implementation	System log	Documentation relating to systems implementation	DESTROY – 2 years after system no longer in use	Thurrock Council
Integration and interfaces	System log	Documentation in relation to data conversion, data matching, data mapping and system interfacing	DESTROY – 2 years after system no longer in use	Thurrock Council
Maintenance	System log	Documentation relating to the maintenance and support of software and systems. Includes website	DESTROY – 2 years after system no longer in use	Thurrock Council
Manuals	System log	Manuals and user information relating to specific systems and software	DESTROY – 2 years after system no longer in use	Thurrock Council
Information Management				
Access to Information				
Data protection		Process around the request under data protection	DESTROY – when information no longer required	Thurrock Council
Data protection		Process of notifying the Information Commissioner on data held	DESTROY – 3 years after previous notification	Thurrock Council
Environmental information	Information requests	Statistical data about the number of requests you answered and their outcomes etc... Details of access decisions	DESTROY – 10 years after data created	The National Archives Retention and Disposal Guidance 14.
Environmental information	Information requests	Information subject to an EIR request but scheduled for disposal	DESTROY – 6 months after last correspondence	The National Archives Retention and Disposal Guidance 14.
Environmental information	Information requests	Case file records detailing the EIR request, the consideration of possible exemptions and subsequent appeals	DESTROY – 3 years after date of creation	The National Archives Retention and Disposal Guidance 14.

Environmental information	Information requests	Procedures for handling EIR requests and other documents regarding practical implementation on EIR	DESTROY – 5 years after procedures have been superseded	The National Archives Retention and Disposal Guidance 14.
Freedom of information	Information requests	Statistical data about the number of requests you answered and their outcomes etc... Details of access decisions	DESTROY – 10 years after data created	The National Archives Retention and Disposal Guidance 14.
Freedom of information	Information requests	Information subject to a FOI request but scheduled for disposal	DESTROY – 6 months after last correspondence	The National Archives Retention and Disposal Guidance 14.
Freedom of information	Information requests	Case file records detailing to FOI request, the consideration of possible exemptions and subsequent appeals	DESTROY – 3 years after date of creation	The National Archives Retention and Disposal Guidance 14.
Freedom of information	Information requests	Procedures for handling FOI requests and other documents regarding practical implementation of FOI	DESTROY – 5 years after procedures have been superseded	The National Archives Retention and Disposal Guidance 14.
Freedom of information	Information requests	The publication scheme that is required under to Freedom of Information Act 2000	PERMANENT- offer to archivist	Thurrock Council
Archives				
Archives management		The consolidated listing of all records held by the authority	PERMANENT – Offer to archivist	Records Management Society of Great Britain
Knowledge Management				
Information asset management		List of information assets	PERMANENT – Offer to archivist	Records Management Society of Great Britain
Information asset management		Information relating to an audit of records of various types	PERMANENT – Offer to archivist	The National Archives Retention and Disposal Guidance 9.
Information asset management		Information in regards to circulation lists, address books etc...	PERMANENT – Offer to archivist	Records Management Society of Great Britain
Records Management				
Compliance		Information and data standards as used by the authority, e.g. E-GMS, planning data set etc...	DESTROY – when new issue has been agreed and circulated	The National Archives Retention and Disposal Guidance 9.
Forms development		Standard templates	DESTROY – 5 years after procedures have been superseded	Local Decision

Forms development		Manual and electronic forms design	DESTROY – 5 years after procedures have been superseded	Local Decision
Image capture		Audio visual library information	Refer to specific areas	Local Decision
Retention scheduling	Disposal Schedules	Information regarding disposal of the council's records	RETAIN –permanently	The National Archives Retention and Disposal Guidance 9.
Tracking		Information regarding tracing and tracing the movement of information from records, archives and libraries	PERMANENT – offer to archivist unless specific legislation requires otherwise	Limitations Act 1980
Registration				
Statutory registers		Statutory data registers	PERMANENT – offer to archivist unless specific legislation requires otherwise	Limitations Act 1980
Legal Services				
Advice				
Advice to the public		Community legal services	DESTROY – 6 years from date of last action	Limitations Act 1980
Provision of legal advise		Providing advice to clients and services which are legally privileged relating to all aspects of the system	DESTROY – 6 years after last action	Retention Guidelines for Local Authorities No. 4.2
Witness support		Witness support schemes	DESTROY – 3 months from date of last action	Avon and Somerset Police
Bylaws				
Enactment		The process of making local laws	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 9.22
Enforcement		The process of administering and enforcing bylaws	DESTROY – 2 years after matter is concluded	Retention Guidelines for Local Authorities No. 9.23
Land and Highways				
Acquisition		Documentation relating to the process of acquiring land in relation to roads	RETAIN – for life of building plus 12 years – offer material re significant/major properties to archivist	Records Management Society of Great Britain
Disposal		Disposal of land associated with the highway	DESTROY – 12 years after disposal date or when obligations cease– offer	The National Archives Retention and Disposal Guidance 1.

			material re significant/major properties to archivist	
Land Registration				
Land charges		Searches and title investigations	DESTROY – 6 years after last action	Limitations Act 1980
Land charges		Legal documentation relating to land charges	DESTROY – 6 years after last action	Limitations Act 1980
Litigation				
Civil	Case files	Civil litigation	DESTROY – 7 years after last action, major litigation offer to archivist for review	Retention Guidelines for Local Authorities No. 4.1
Commercial	Case files	Commercial litigation	DESTROY – 7 years after last action, major litigation offer to archivist for review	Retention Guidelines for Local Authorities No. 4.1
Criminal	Case files	Criminal litigation	DESTROY – 7 years after last action, major litigation offer to archivist for review	Retention Guidelines for Local Authorities No. 4.1
Debt recovery	Case files	Debt recovery	DESTROY – 7 years after last action, major litigation offer to archivist for review	Retention Guidelines for Local Authorities No. 4.1
Precedent cases	Case file	Judgments relied on to fight current cases – setting standards to work within	PERMANENT – offer to archivist	Records Management Society of Great Britain
Management of Legal Activities				
Archive deposits		Legal documentation relating to archive depositors	PERMANENT – offer to archivist	Records Management Society of Great Britain
Agreements		Agreements including non-contractual agreements between public bodies	DESTROY – 6 years after agreement ends	Retention Guidelines for Local Authorities No. 4.3
Conveyancing	Deeds	Commercial and other leases, Title investigations, Disposal of Freehold and Leasehold properties, Right to Buy applications etc…	DESTROY – 12 years after closure	Retention Guidelines for Local Authorities No. 4.4
Conveyancing	Deeds	Private right of way, right to light (an easement benefits on piece of land	DESTROY – 12 years after closure	Limitations Act 1980

		by exercising rights over another piece of land owned by another) procedures are in place to ensure the efficient and lawful use of easements		
Conveyancing		Documentation relating to the rental agreements of council buildings, council houses, allotments, garages, commercial properties, wayleaves and land.	DESTROY – 12 years from termination of tenancy	Retention Guidelines for Local Authorities No. 3.28
Copyright		Information on who owns the information. For example, ensuring no breach of copyright	DESTROY – 6 years after agreement	Local Decision
Drafting		A range of pro-forma legal agreements used in all areas of law	DESTROY – once final document is complete	Eastbourne Borough Council
Trusts		Documentation related to legal service and trusts	RETAIN – 25 years before considering disposal	Eastbourne Borough Council
Planning Controls				
Certificate of Lawful Use of Development		Lawful development certificate	PERMANENT – offer to archivist	Town and Country Planning Act 1990
Certificate of Lawful Use or Development		Files relating to Lawful Development Certificate	DESTROY – 12 years from date of agreement	Limitations Act 1980
Section 106 agreements		Section 106 agreement	PERMANENT – offer to archivist	Town and Country Planning Act 1990
Section 106 agreements		Files relating to a planning obligation or legal agreement made under section 106 Town and County Planning Act 1990	DESTROY – 12 years from date of agreement	Limitations Act 1980
Leisure and Culture				
Allotments				
Allotments		Information relating to the provision of allotments	DESTROY – 6 years from termination	Limitations Act 1980
Archives				
Archive development		Archive development records	RETAIN – for lifetime of the deposit	Staffordshire County Council

Cataloguing		The consolidated listing archival resources available to the public	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 2.11
Deposits		Depositor records	RETAIN – for lifetime of deposit	Staffordshire County Council
Loans		Documentation related to loans within the archive	RETAIN – for lifetime of deposit	Staffordshire County Council
Membership		Documentation related to membership of the archive	DESTROY – 1 year from termination of membership	Lincolnshire County Council
Research		Information relating to research services	DESTROY – 6 years from end of current financial year	Staffordshire County Council
Arts				
Arts development		Documentation related to art development	DESTROY – After 4 years depending on scale of project	Eastbourne Borough Council
Clubs and societies		Documentation related to care within clubs and societies	PERMANENT – offer to archivist	Eastbourne Borough Council
Community Facilities				
Equipment		Hire items of equipment for events	PERMANENT – offer to archivist after 1 year	Staffordshire Borough Council
Grants		Provision of grants to village halls and other local facilities	DESTROY – 3 years from expiry of grant	Lincolnshire County Council
Venues		Details on any venues to local authority may have available for private/business hire	PERMANENT – offer to archivist	Staffordshire County Council
Leisure Promotion				
Countryside events		Information related to countryside programmes and events	RETAIN – 2 years from end of event	Eastbourne Borough Council
Exhibitions		Exhibitions arranged by or held on Council premises	DESTROY – 6 years from end of current financial year	Staffordshire County Council
Inclusion		Activities and events targeted at specific groups of people	RETAIN – 3 years from end of event	Eastbourne Borough Council
Parks and garden events		Information related to parks and gardens	Retain – 2 years from end of event	Eastbourne Borough Council
Play scheme		Documentation relating to play schemes	DESTROY – once obsolete	Eastbourne Borough Council

Libraries				
Book ordering		Documentation relating to book ordering	DESTROY – 6 years from end of current financial year	Staffordshire County Council
Bookings		Documentation relating to conventional library bookings	DESTROY - after 6 years	Staffordshire County Council
Bookings		Documentation relating to web-based library bookings	DESTROY – after 6 years	Staffordshire County Council
Catalogue		Documentation relating to the library catalogue	DESTROY – 2 years after administrative use concluded	Thurrock Council
Fines		Documentation relating to library fines including guidelines and procedures	DESTROY – 7 years from end of recovery action	Gedling Borough Council
Library development		Documentation relating to library development	DESTROY – 6 years after administrative use concluded	Staffordshire County Council
Loans		Documentation relating to library loans	DESTROY – 1 year after return of item	Staffordshire County Council
Membership		Documentation relating to library membership	DESTROY – 1 year from termination of membership (unless debtor)	Eastbourne Borough Council
Support for schools		School library services	DESTROY - 6 years from end of current academic year	Staffordshire County Council
Museums				
Deposit		Documentation relating to a depositor within a museum	RETAIN – for lifetime of deposit	Staffordshire County Council
Loans		Documentation regarding museums loans	RETAIN – for lifetime of deposit	Staffordshire County Council
Museum catalogue		Documentation regarding museum catalogue	RETAIN – for lifetime of deposit	Staffordshire County Council
Museums development		Documentation regarding museum development	RETAIN – for lifetime of deposit	Staffordshire County Council
Parks and Open Spaces				
Maintenance		Maintenance of parks and open spaces	RETAIN – 21 years before considering disposal	Eastbourne Borough Council
Playgrounds		Playgrounds and play areas	RETAIN – 21 years before considering disposal	Eastbourne Borough Council

Sports Facilities				
Bookings		Documentation related to general sport bookings	RETAIN – 5 years then consider for destruction	Eastbourne Borough Council
Bookings		Documentation related to the booking of specific sporting facilities	RETAIN – 5 years then consider disposal	Eastbourne Borough Council
Bookings		Documentation related to membership of sports classes and training regime	RETAIN – 5 years then consider disposal	Eastbourne Borough Council
Equipment hire		Details of sports equipment that is available for hire	RETAIN – 5 years then consider disposal	Eastbourne Borough Council
Membership		Information related to general sports membership	DESTROY – once documents become obsolete	Eastbourne Borough Council
Membership		Information related to the membership of golf clubs	DESTROY – once document become obsolete	Eastbourne Borough Council
Membership		Information regarding to leisure centre membership	DESTROY – once documents become obsolete	Eastbourne Borough Council
Sports				
Sports development		Information related to sport development programmes	RETAIN – 5 years before considering disposal	Eastbourne Borough Council
Clubs and societies		Documentation associated with sports clubs	RETAIN – 5 years then consider destruction	Eastbourne Borough Council
Tourism				
Tourist accommodation		Information about tourist facilities in the local area. Includes lists of visitors' accommodation available locally and information relating to the accreditation of such accommodation	DESTROY – After 6 years	Eastbourne Borough Council
Tourist accommodation		Process of accrediting visitor accommodation	DESTROY – After 6 years	Eastbourne Borough Council
Tourist accommodation		Information related to tourist accommodation registers	DESTROY – After 6 years	Eastbourne Borough Council
Visitor information		Leisure and cultural services provided or supported by the council for the community. Specifically includes visitor attractions	RETAIN – 2 years before considering disposal	Staffordshire County Council

Visitor information		Maps, directions and locations available for public leisure	RETAIN – 2 years before considering disposal	Staffordshire County Council
Management				
Ceremonial				
Civic and Royal events		Documentation relating to civic functions or visits by royalty to the local area	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 2.24
Civic and Royal events		Information on planning and organising an event	DESTROY – 7 years after use	Retention Guidelines for Local Authorities No. 2.25
Corporate gifts		Documentation relating to the provision of corporate gifts	RETAIN – 4 years before considering disposal	Eastbourne Borough Council
Communication Support				
Interpreting and translation		Language translation services	DESTROY - years from last action	Staffordshire County Council
Mail processing		Processes connected with handling mail and associated communications	DESTROY - 1 year from date of last action	Local Decision
Publication		Guides, books and other publications that the council makes available on a chargeable basis	DESTROY – 3 years from date of last action	Lancaster City Council
Publications received		Information management publications	DESTROY – 3 years from date of last action	Lancaster City Council
Staff communications		Staff communication documentation	DESTROY – 1 year from date of last action	Eastbourne Borough Council
Corporate Communication				
Campaigns		Documentation relating to the promotion of a business through publicity campaigns	PERMANENT – offer to archivist	Essex County Council
Corporate branding		Documentation relating to the process of creating and the use of a corporate image and relevant guidance within the authority	OFFER to archivist for review	Local Decision
Corporate publicity		Documentation relating to corporate publicity	PERMANENT – offer to archivist	Essex County Council
Graphic design		Documentation relating to graphic design requirements of the authority	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 2.19

Marketing		Documentation relating to the marketing of the council or a specific function or service	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 2.23
Media cuttings		Compilation of media in which the local area or authority is mentioned	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 2.22
Media liaisons		Documentation relating to liaison between the council and local media	DESTROY – 3 years from closure	Retention Guidelines for Local Authorities No. 2.21
Media releases		Information release to the media	DESTROY – 7 years from date of last action	The National Archives Retention and Disposal Guidance 8.
Media releases		Documentation relating to media releases the promotion of business	DESTROY – 3 months from date of last action	The National Archives Retention and Disposal Guidance 8.
Public relations		Documentation relating to public relations	DESTROY – 3 years from date of last action	Lancaster City Council
Public relations		Media reports	DESTROY – 3 years from date of last action	The National Archives Retention and Disposal Guidance 8.
Public relations		Published work	DESTROY – after use is concluded – one copy to archive	Retention Guidelines for Local Authorities No. 2.20
Public relations		Statistics	DESTROY – 10 years after use is concluded	Lancaster City Council
Enquiries and Complaints				
Appeals		Formal complaints received and response to the complaints. Includes the FOI, EIR and the data protection complaints process	DESTROY – 5 years after use is concluded	Local Decision
Complaints		Complaints which result in significant changes of policy	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 2.14
Complaints		Summary form of complaints	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 2.13
Complaints		Identification of a specific complaints to the council	DESTROY – 3 years after last action	The National Archives Retention and Disposal Guidance 7.
Complaints to Ombudsman	Complaint files	Documentation related to Ombudsman complaints	DESTROY – 10 years after concluded	The National Archives Retention and Disposal Guidance 7.
Compliments		Compliments and comments and response received and response to	RETAIN – 6 years from end of administrative use	Eastbourne Borough Council

		them		
Customer profiling		Information provided by an individual or organisation that includes personal preferences	DESTROY – 1 year from date of last action	Eastbourne Borough Council
Customer satisfaction		Feedback on council performance in relation to services or other aspects of council business	DESTROY – 5 years from date of last action	The National Archives Retention and Disposal Guidance 7.
Stage 1 complaints	Complaint files	Documents related to stage 1 complaints	DESTROY – 2 years after concluded	Retention Guidelines for Local Authorities No. 2.16
Stage 2 complaints	Complaint files	Documents related to stage 2 complaints	DESTROY – 6 years after concluded	Retention Guidelines for Local Authorities No. 2.15
External Audits				
Audits		Documentation on audits - The external activities (usually carried out by a district audit) associated with officially checking financial, quality assurance and operational records to ensure they have been kept and maintained in accordance with agreed or legislated standards and correctly record the events, processes and business of the organisation in a specified period	DESTROY – 6 years from date of last action	The National Archives Retention and Disposal Guidance 10.
Preparing Business				
Meetings		Information regarding meetings	PERMANENT – offer to archivist	Eastbourne Borough Council
Officer representation		Documentation relating to officer representation	DESTROY – 3 years from date of last action	Eastbourne Borough Council
Partnership and agency working	Business for partnership and agencies where local authority owns the record	Documentation relating to agency working	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 1.6

Partnership and agency working	Business for partnership and agencies where local authority does not own the record	Documentation relating to agency working	DESTROY – 3 years from last action	Retention Guidelines for Local Authorities No. 1.7
Project Management				
Closure	Project files – Lessons learned	Information obtained by reviewing the project	DESTROY – 6 years from completion of the project	Limitation Act 1980
Governance	Project files – Project Initiation document	Document created at the start of the project to indicate how it will be run	DESTROY – 10 years after completion of project	The National Archives Retention and Disposal Guidance 6.
Governance	Project files – Unit or Team Plans	Planning documentation	DESTROY – 10 years after completion of project	The National Archives Retention and Disposal Guidance 6.
Initiation and delivery	Project files – Issues Log	Unforeseen events requiring action	DESTROY – 6 years from completion of the project	Limitation Act 1980
Start up	Project files – Business Case	Information related to planning a business operation or service	DESTROY – 10 years after completion of project	The National Archives Retention and Disposal Guidance 6.
Quality and Performance				
Assessments		Assessments	DESTROY – 2 years from closure	Retention Guidelines for Local Authorities No. 2.18
Best value reviews		Best value reviews	DESTROY – 5 years from closure	Retention Guidelines for Local Authorities No. 2.17
Inspections		Documentation relating to the external inspections received by the authority in relation to corporate or service specific performance management	DESTROY – 3 years from date of last action	Eastbourne Borough Council
Process mapping		Information relating to specific quality initiatives such as ISO 9000	DESTROY – 3 years from date of last action	Eastbourne Borough Council

Statutory Returns				
Reports to government		The process of preparing information to be passed on to central government as part of statutory requirements	DESTROY – 7 years from closure	Retention Guidelines for Local Authorities No. 2.5
Strategic Planning				
Business cases		Information related to identifying a need or requirement for a business or service process	PERMANENT – offer the archivist	Eastbourne Borough Council
Corporate initiatives		Documentation relating to corporate initiatives	DESTROY – 5 years after initiative ends	Thurrock Council
Organisational structure		Organisational structure of the school library service	PERMANENT – offer to archivist	Eastbourne Borough Council
Policies and procedures		Documentation relating to policies and procedures of the council	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 2.6
Public consultation		The process of consultation with the public	DESTROY -1 year from closure	Retention Guidelines for Local Authorities No. 2.9
Public consultation		The process of consultation with the public	DESTROY – 5 years from closure	Retention Guidelines for Local Authorities No. 2.8
Service level agreements		Information relating to agreements made between separate internal units or teams on a contractual basis	DESTROY – 2 years from expiration of terms	Eastbourne Borough Council
Planning and Building Control				
Building Control				
Application processing		Application files containing application, validation notice, correspondence, drawings, location plans, structural calculations, decision notices, record cards, inspection reports and contravention notices	DESTROY – after 3 years if rescinded otherwise PERMANENT – offer to archivist	Building Act 1984
Application processing		Correspondence before an application is submitted	DESTROY – 15 years from date of last action	Building Act 1984
Building regulations		Documentation relating to building standards and inspection	DESTROY – 3 years from date of compliance with	Wychavon District Council

			enforcement notice	
Registration		Building control register sheets	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 10.8
Unauthorised works		Information relating to unauthorised works	DESTROY – 3 years after the removal of or alteration to the unauthorised work	Local Decision
Covenant Controls				
Policies		Information relating to policies	DESTROY – 6 years after being superseded	Local Decision
Covenant controls		Covenant control files containing applications, correspondence, drawing and notices	PERMANENT – offer to archivist	Local Decision
Development Control				
Application processing		Documentation related to planning appeals	DESTROY – 6 years from conclusion of appeal	Limitations Act 1980
Application processing		Application files containing application letters and forms, certificates, locations plans, drawings, site correspondence, reports, photographs and s. 106 agreements	DESTROY – 10 years after result announced	The National Archives Retention and Disposal Guidance 1.
Application processing		Decision notices on planning applications	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 10.6
Application processing		Pre application discussion documentation relating to a specific building	DESTROY – 15 years from last action	Thurrock Council
Conservation areas		Information regarding specific sites and monuments	DESTROY – 15 years from last action	Retention Guidelines for Local Authorities No. 10.3
Enforcement		The enforcement of demolition guidelines and laws	DESTROY – 3 years after compliance with enforcement notice	Retention Guidelines for Local Authorities No. 10.13
Hedges		Actions to resolve disputes over evergreen hedges	DESTROY – 5 years from date of last action	Eastbourne Borough Council
Registration		Register sheets including application register, decision register,	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 10.6

		consultation register, enforcement register, s.106 register, tree works register		
Planning obligations		Documentation relating to planning obligations	PERMANENT – offer to archivist	Eastbourne Borough Council
Tree		Information containing reference to listed tree life	DESTROY – 5 years after application decision	Thurrock Council
Tree		Tree preservation orders	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 10.6
Forward Planning				
Economic regeneration		Information on activities to support local economic regeneration in the local area	DESTROY – 12 years from date of last action	Staffordshire County Council
Heritage listing		The consolidated list of heritage buildings and sites	PERMANENT – offer to archivist	Wychavon District Council
Housing development		Documentation related to social housing development	DESTROY – 6 years from completion of the project	Eastbourne Borough Council
Local plan		Local planning documentation	PERMANENT – offer to archivist	Eastbourne Borough Council
National planning policy		National planning policy information	DESTROY – once obsolete	Staffordshire County Council
Natural environment		Information on agriculture, countryside, nature reserves and protected sites	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 10.7
Natural environment		The process of maintaining the countryside and developing open spaces for public amenity	DESTROY – 7 years after administrative use concluded	Retention Guidelines for Local Authorities No. 10.7
Planning policy		Planning policy documentation in relation to specific buildings	DESTROY – 5 years from date of last action	Eastbourne Borough Council
Planning schemes		The process of receiving, considering and responding to submissions and objections to planning schemes and amendments	DESTROY – 15 years after decision. Offer controversial or high profile schemes to Archivist	Retention Guidelines for Local Authorities No. 10.5
Regional plan		Regional planning information	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 10.4
Regional plan		Mineral plans	PERMANENT – offer to	Retention Guidelines for Local

			archivist	Authorities No. 10.4
Regional plan		Waste plans	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 10.4
Regional plan		Structure plans	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 10.1
Sustainable development		Information on biodiversity, flooding and pollution	DESTROY – 10 years after completion of the project	The National Archives Retention and Disposal Guidance 6.
Urban centre planning		Town and city centre planning documentation	PERMANENT – offer to archivist	Records Management Society of Great Britain
Procurement				
Contracting				
Approved suppliers		Maintaining a list of approved suppliers to the local authority	DESTROY – once superseded	The National Archives Retention and Disposal Guidance 5.
Contract awards		Information of who was successful in obtaining a contract or contracts we undertake for others	DESTROY – 6 years if value less than £50,000 or 12 years if over £50,000 once all contractual obligations concluded	Lancaster City Council
Contract awards	Contract files	Contract documents and any contact amendments	DESTROY – 6 years after the term of the contract has expired	Retention Guidelines for Local Authorities No. 4.6
Contract awards	Contract files	Contact documents and any contract amendments where contract is under seal	DESTROY – 12 years after the term of the contract has expired	Retention Guidelines for Local Authorities No. 4.6
Contact awards	Contract files	Negotiation files related to specific contracts	DESTROY – 1 year after the term of the contract has expired	Retention Guidelines for Local Authorities No. 4.11
Contract awards	Contract files	Performance monitoring and review of awarded contracts	DESTROY – 2 years after the term of the contract has expired	Retention Guidelines for Local Authorities No. 4.13
Contract management		The monitoring of contracts	DESTROY – 6 years if value less than £50,000 or 12 years if over £50,000 once all contractual obligations concluded	Lancaster City Council

Requisition		Documentation on non tendered contracts	DESTROY – 7 years after the end of the financial year	Retention Guidelines for Local Authorities No. 7.3
Market Information				
Product evaluation		Information on any products evaluated	DESTROY – 6 years from last action	Lancaster City Council
Product information		Information held by the organisation on products with a view to purchase at a later stage (e.g. product literature)	DESTROY – 6 years from last action	Lancaster City Council
Tendering				
Tenders	Tender files	Tender issuing and return	DESTROY – 1 year after start of contract	Retention Guidelines for Local Authorities No. 4.7
Tenders	Tender files	Tendering of contracts, responses and their evaluation	DESTROY – 6 years from termination	Limitation Act 1980
Tenders	Tender files	The process of calling for expression of interest	DESTROY – 2 years after contract let or not proceeded with	Retention Guidelines for Local Authorities No. 4.5
Tenders	Tender files	Tendering of contracts, responses and their evaluation for contracts under seal	DESTROY – 12 years after the term of the contract has expired	Limitations Act 1980
Tenders	Tender files	Documentation relating to unsuccessful tenders	DESTROY – 1 year after start of contract	Retention Guidelines for Local Authorities No. 4.10
Tendering policies		Documentation relating to tendering policies	DESTROY – 6 years from date of last review, 25 years for Trunk Road Schemes	Limitations Act 1980
Registration and Coroners				
Inquiries into Deaths				
Coroners inquests	Case files	Inquiries leading to an inquest	PERMANENT – offer to archivist	The National Archives Retention and Disposal Guidance 13.
Investigations		Inquiries not proceeding to an inquest	DESTROY – 15 years after last action	Operational Selection Policy OSP6: Records created by and relating to Coroners 1970 - 2000 2005 and 2007
Registration		Register of reported deaths	DESTROY – 15 years after last action	Operational Selection Policy OSP6: Records created by and relating to

				Coroners 1970 - 2000 2005 and 2007
Marriage Services				
Conducting a marriage service		Process of arranging and carrying out a marriage service	DESTROY – 3 years after last action	Retention Guidelines for Local Authorities No. 5.3
Registration		Register of places approved to hold wedding services	REVIEW – 3 years after creation	Licensing Act 2003
Registration of Births, Marriages and Deaths				
Advice and support		Supplying advice and support on arrangements that need to be made	DESTROY – 5 years from date of last action	Nottingham City Council
Certification		Records of applications for copies of certificates	DESTROY – 7 years from date of last action	Nottingham City Council
Certification		Issuing of certificates	DESTROY – 7 years after last action	Retention Guidelines for Local Authorities No. 5.2
Notification		Process of arranging for a marriage notice to be displayed. Weddings banns	DESTROY – 2 years after last action	Retention Guidelines for Local Authorities No. 5.4
Registration		The process of registering a marriage	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 5.1
Registration		Process of registering a birth	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 5.1
Registration		Process of registering citizenship	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 5.1
Registration		Process of registering the death of individuals	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 5.1
Treasure Trove				
Inquests		Process of investigation of treasure trove	DESTROY – 2 years after last action	The National Archives Retention and Disposal Guidance 13.
Risk Management and Insurance				
Claims				
Claims processing		Documentation relating to claims made against the council	DESTROY – 6 years after all obligations and entitlements are concluded	Limitations Act 1980
Insuring Against Loss				

Insurance		Documentation relating to insurance policies	DESTROY – 7 years after the terms of the policy have expired	Retention Guidelines for Local Authorities No. 8.19
Insurance		Renewal information	DESTROY – 5 years after the policy has been renewed	Retention Guidelines for Local Authorities No. 8.20
Insurance		Summary of arrangements relating to insurance	PERMANENT - offer to archivist	Retention Guidelines for Local Authorities No. 8.18
Risk Management				
Business Continuity Planning		Documentation relating to business continuity in the event of a disaster or unforeseen event. Includes disaster recovery and business resilience plans.	DESTROY – once superseded	Staffordshire County Council
Education		Campaigns related to risk management	DESTROY – 2 years from date of last action	Staffordshire County Council
Risk assessment		Consolidated listing of, and assessment of risks	DESTROY – 3 years from date of last action	Staffordshire County Council
Risk assessment	Documents relating to children	Valuations as park of the risk assessment process	DESTROY – 3 years from date of person turning 18	Staffordshire County Council
Transport and Infrastructure				
Design and Construction				
Roads and Highways		Documentation related to the design and constructions of roads and highways	PERMANENT - offer to archivist	Retention Guidelines for Local Authorities No. 11.7
Traffic Management schemes		Design and construction of highways, traffic management schemes and road signs. Includes feasibility studies.	DESTROY – 25 years from date of last action	Eastbourne Borough Council
Harbours and Waterways				
Boat moorings		Information relating to boats and their moorings	PERMANENT – offer to archivist	Local Decision
Registration		Documentation related to watercraft	PERMANENT – offer to archivist	Local Decision
Highway Development Control				

Highway adoption		Adoption of new highways	PERMANENT - offer to archivist	Retention Guidelines for Local Authorities No. 11.3
Highway extent queries		Handling of highways extents enquiries from solicitors, developers, districts etc…	PERMANENT - offer to archivist	Retention Guidelines for Local Authorities No. 11.2
Highway extinguishment		Extinguishment of highways	DESTROY – 20 years after creation	Highways Act 1980
Notification		Documentation relating to notification to the public of maintenance, changes in status and closures etc…	DESTROY – once superseded	Staffordshire County Council
Planning Control		The process of receiving, considering and responding to submissions and objections to planning schemes and amendments	DESTROY – 7 years after extinguishment. Offer controversial or high profile scheme to archivist	Retention Guidelines for Local Authorities No. 11.4
Road classification		Gazetteer of highways types	DESTROY – 7 years from date of last action	Nottingham City Council
Highway Enforcement				
Advertising hoarding		Documentation related to the control of advertisement hoarding	DESTROY – once obsolete	Staffordshire County Council
Highways		Documentation relating to enforcement of the proper use a maintenance of transport and highways	DESTROY – 3 years after compliance with enforcement notice	Retention Guidelines for Local Authorities No. 11.5
Parking		Enforcement of parking infringement includes both on site and off site	DESTROY – 2 years from date of last action	Gedling Borough Council
Parking fines		Documentation related to parking fines	DESTROY – 1 year from date of last action	Eastbourne Borough Council
Road reinstatement		Documentation related to the reinstatement of roadways	DESTROY – 6 years from date of last action	Local Decision
Scaffolding		Documentation related to the regulation of scaffolding and the enforcement of rules and regulations associated with this	DESTROY – 6 years from date of licence expiration	Staffordshire County Council
Speeding fines		Documentation related to speeding fines	DESTROY – 7 years from end of current financial year	Lincolnshire County Council

Weight limits		Documentation related to the enforcement of weight limits	DESTROY – 7 years from date of last action	Lancaster County Council
Infrastructure Management				
Cycle routes		Provision for cycle routes	DESTROY – 6 years from date of completion	Staffordshire County Council
Geotechnical services		Feasibility studies, desk studies, geotechnical site investigations, site and laboratory testing and contaminated land studies provided by the local authority	DESTROY – 6 years from date of last action	Local Decision
Maintenance		Documentation related to general maintenance of transportation systems	DESTROY – 6 years from date of last action	Staffordshire County Council
Markings and signage		Installation instructions and warning signs	DESTROY – once obsolete	Eastbourne Borough Council
Public conveniences	Job Tickets	Provision of pubic conveniences. Toilets. Maintenance and cleaning	DESTROY – 2 years from date of last action	Eastbourne Borough Council
Service providers		Documentation relating to service providers	DESTROY – 6 years from end of current financial year	Eastbourne Borough Council
Street furniture		Documentation relating to the process of installing and maintaining street furniture: finger posts, litter bins, public seats etc…	DESTROY – 7 Years after last action	Retention Guidelines for Local Authorities No. 11.8
Street naming and numbering		Documentation on the street naming, development naming and property numbering / naming	PERMANENT – offer to archivist	Eastbourne Borough Council
Surveys		Survey data relating to transport and infrastructure	DESTROY – 7 years from end of current financial year	Eastbourne Borough Council
Taxi ranks		Provision of designated taxi ranks	DESTROY – 6 years from date of last action	Local Decision
Public Transport				
Community transport		Transport for members of the community, includes schemes such as 'dial-a-ride', shop mobility, community bus and car schemes	DESTROY – 6 years from date superseded	Staffordshire County Council

Concessions		Information regarding the transport concessions offered to the disabled	DESTROY – 6 years after conclusion	Lancaster City Council
Public transport plan		Information about future plans, public transport routes and timetables	DESTROY – 3 years after superseded or last action	Retention Guidelines for Local Authorities No. 11.11
Timetable		The timetabling of public transportation systems	DESTROY – 7 years from date of last entry	Lincolnshire County Council
Rights of Way				
Enquiries		Enquiries and correspondence from the public concerning rights of way	DESTROY – 1 year from conclusion of enquiry	Staffordshire County Council
Locations		Information including maps defining the locations and routes of rights of way.	PERMANENT – offer to archivist	Thurrock Council
Orders		Orders creating public rights of way	DESTROY – 6 years from conclusion of transaction	Thurrock Council
Planning applications		Management of the council's responses from a rights of way management perspective to planning applications and proposals	DESTROY – 7 years from date of last action	Eastbourne Borough Council
Ploughing and cropping		Regulation of ploughing and cropping on public rights of way	RETAIN – until end of operational use	Kent County Council
Searches		Rights of way searchers carried out by the council	DESTROY – 1 year from conclusion of search	Staffordshire County Council
Road Maintenance				
Bridge inspections		Regular inspections of bridges on highways	DESTROY – 12 years from date of last action	Eastbourne Borough Council
Drains and gullies		Keeping drains and gullies clear and provision of advice on drainage	DESTROY – 6 years from date of last action	Staffordshire Borough Council
Emergency maintenance		Documentation related to emergency maintenance	DESTROY – 12 years after action completed	Retention Guidelines for Local Authorities No. 11.9
Hazard removal		Removal of hazards on the road. Including removal of dead animals etc...	DESTROY – 12 years from date of last action	Gedling Borough Council
Inspections		Documentation relating to inspection of adopted highways	DESTROY – 12 years from date of last action	Eastbourne Borough Council
Kerbs		Vehicle crossovers	DESTROY – 12 years from	Eastbourne Borough Council

			date of last action	
Planned maintenance		Documentation relating to unplanned and planned maintenance	DESTROY – 12 years after action completed	Retention Guidelines for Local Authorities No. 11.9
Scheduled maintenance		Documentation related to scheduled maintenance	DESTROY – 12 years after action completed	Retention Guidelines for Local Authorities No. 11.9
Verge maintenance		Documentation related to the maintenance of verges	DESTROY – 12 years from date of last action	Eastbourne Borough Council
Road Safety				
Accident investigations		Investigations into road traffic accidents for the purpose of improving road safety MOT testing of vehicles by accredited council garages	DESTROY – 7 years after use	Thurrock Council
MOT testing		MOT testing of vehicles by accredited council garages	DESTROY – 6 years from date of test	Limitations Act 1980
Road safety awareness		Documentation relating to road safety awareness	DESTROY – 2 years from date of last action	Staffordshire County Council
Safety audits		Audit / inspections of highways from a road safety perspective	DESTROY – 7 years after use	Thurrock Council
School crossing patrols		Documentation relating to school crossing patrols	DESTROY – 7 years from date of last action	Records Management Society of Great Britain
Speed cameras		Includes information on the reason for the siting of the camera, any settings etc...	DESTROY – 6 years from date agreement superseded	Staffordshire County Council
School Transport				
School transport services		Documentation relating to school transport service	DESTROY – 6 years from date of last action	Limitation Act 1980
Traffic Management				
Abnormal loads		Consent for moving an abnormal load	DESTROY – 2 years after consent given	Thurrock Council
Gritting and snow clearance		Keeping roads and pavements clear when weather conditions may prove hazardous	DESTROY – 10 years from date of last action	Staffordshire County Council
Monitoring		Includes the monitoring of highway, transport and traffic use	DESTROY – 7 years from date of last action	Eastbourne Borough Council

Parking		Documentation relating to parking permits, parking schemes, skips, scaffolding etc. Includes information relating to the development and management of controlled parking zones	DESTROY – 7 years from date of last action	Gedling Borough Council
Parking sites		Documentation relating to the specifics of parking sites	PERMANENT – offer to archivist	Gedling Borough Council
School routes		The activity of planning and programming the continued safety of school routes	DESTROY – 7 years from date of last action	Staffordshire County Council
Street lighting		The activity of planning and programming the continued effectiveness of street based lighting	DESTROY – 7 years from date of last action	Eastbourne Borough Council
Traffic calming		The management and control of traffic calming measures	DESTROY – 7 years from date of last action	Eastbourne Borough Council
Traffic reduction		The activity of planning and programming the continued flow, diversion or reduction of traffic	DESTROY – 7 years from date of last action	Eastbourne Borough Council
Traffic orders		Traffic management and parking requires to be regulated by various statutory orders	DESTROY – 7 years after action completed	Retention Guidelines for Local Authorities No. 11.6
Traffic orders		Implementation of road traffic orders	DESTROY – 5 years after action completed	Thurrock Council
Traffic orders		The planning and investigation of road traffic orders	DESTROY – 5 years after action completed	Thurrock Council
Transport Planning				
Development control		Documentation associated with the approval of planning applications which affect this section	PERMANENT – offer to archivist	Eastbourne Borough Council
Strategy and planning		Development of transport strategy	DESTROY – 5 years from date of last action	Eastbourne Borough Council
Strategy and planning		The planning of transport issues	PERMANENT – offer to archivist	Retention Guidelines for Local Authorities No. 11.1
Transport modelling		The carrying out of transport	DESTROY – 2 years after	Thurrock Council

		modelling projects	last use	
Transport modelling		Traffic census data	DESTROY – 2 years after last use	Thurrock Council
Travel plans		Employer travel plans	DESTROY – 2 years after last use	Lincolnshire County Council
Travel plans		School travel plans	DESTROY – 7 years from date of last action	Lincolnshire County Council
Waste Management				
Fly Tipping				
Fly tipping		Dumped rubbish which varies in size from a single bin bag to several truck loads of construction waste	DESTROY – 2 years from date of last action	Eastbourne Borough Council
Street Cleaning				
Pest control		The management and control of pests	DESTROY – 3 years from date of last action	Eastbourne Borough Council
Road cleansing		The cleaning of public roadways	DESTROY – 5 years from date of last action	Lincolnshire County Council
Waste Collection				
Abandoned vehicles		A vehicle which deemed to have been abandoned by its owner, as defined in the Refuse Disposal Amenity act 1978 and the Clean Neighbourhoods Act 2005	DESTROY – 2 years after creation	Retention Guidelines for Local Authorities No. 9.26
Bulk		The disposal of commercial waste, as defined in the Environmental Protection Act 1990	DESTROY – 3 years after creation	The Hazardous Waste (England and Wales) Regulations 2005 No. 894
Controlled		The disposal of hazardous waste as defined in the Hazardous Waste Directive 2005 and the European Waste Catalogue	DESTROY – 3 years after creation	The Hazardous Waste (England and Wales) Regulations 2005 No. 894
Domestic		The process of arranging the collection or transportation of home care waste	DESTROY – 3 years after creation	The Hazardous Waste (England and Wales) Regulations 2005 No. 894
Trade		The process of arranging the collection or transportation of trade	DESTROY – 3 years after creation	The Hazardous Waste (England and Wales) Regulations 2005 No. 894

		waste		
Waste Disposal				
Waste sites	Management of sites	Information on waste disposal sites and their management	DESTROY – 3 years after creation	The Hazardous Waste (England and Wales) Regulations 2005 No. 894
Waste sites	Short term storage	Information on sites used for the short term storage of waste	DESTROY – 2 years after creation	The Environmental Protection (Duty of Care) Regulations 1991 No. 2839
Waste sites	Equipment	Information on the equipment installed at waste sites and its operation	DESTROY – 3 years after creation	The Hazardous Waste (England and Wales) Regulations 2005 No. 894
Waste sites	Inspections	Records of inspections of waste sites	DESTROY – 3 years after creation	The Hazardous Waste (England and Wales) Regulations 2005 No. 894
Waste sites	Permits	Permits issued covering the use of waste sites	DESTROY – 3 years after creation	The Hazardous Waste (England and Wales) Regulations 2005 No. 894
Waste sites development	Waste site plans	A plan held by local and regional authorities detailing the provisions for current and future waste management activities	DESTROY – 3 years after creation	The Hazardous Waste (England and Wales) Regulations 2005 No. 894
Waste Reduction				
Composting		The treatment of biodegradable waste, either aerobically or anaerobically to produce a product that can be used as either compost or a soil improver	DESTROY – 2 years after creation	The Environmental Protection (Duty of Care) Regulations 1991 No. 2839
Recycling		The establishment of pubic recycling receptacles	DESTROY – 2 years after creation	The Environmental Protection (Duty of Care) Regulations 1991 No. 2839

APPENDIX 10

ACCESS AND SECURITY PROTOCOL

1. POLICY STATEMENT

1.1 Tameside Metropolitan Borough Council (TMBC) will establish specific requirements for protecting information and information systems against unauthorised access.

1.2 TMBC will effectively communicate the need for information and information system access control.

2. INTRODUCTION

2.1 Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of TMBC which must be managed with care.

2.2 Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

2.3 Formal procedures must control how access to information is granted and how such access is changed.

2.4 This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

3. SCOPE

3.1 This Access Control Policy outlines the framework for the management of Access Control within Tameside Metropolitan Borough Council.

3.2 The Access Control Policy applies to all employees (including system support staff with access to privileged administrative passwords), Members of the Council, temporary staff, contractual third parties, partners or agents of the Council who have access to any Information Systems or information for TMBC purposes.

3.3 Access control rules and procedures are required to regulate who can access TMBC information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing TMBC information in any format, and on any device.

4. USER ACCESS MANAGEMENT

4.1 *Access Control*

4.1.1 Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed by TMBC.

4.1.2 Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

4.1.3 User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

4.2 *User Registration*

4.2.1 A request for access to the Council's computer systems must first be submitted to the IT Service Desk for approval. Applications for access must only be submitted if approval has been gained from the line manager

4.2.2 When an employee leaves the Council, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the line manager to request the suspension of the access rights via the IT Service Desk

4.3 *User Responsibilities*

4.3.1 It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems by:

- Following the Password Policy Statements outlined in Section 10.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing the IT Service Desk of any changes to their role and access requirements.

5. NETWORK ACCESS CONTROL

5.1 The use of modems on non-Council owned computers connected to the Council's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from IT before connecting any equipment to the Council's network.

6. USER AUTHENTICATION FOR EXTERNAL CONNECTIONS

6.1 Where remote access to the TMBC network is required, an application must be made via the IT. Remote access to the network must be secured by two factor authentication consisting of a username and one other component, for example encrypted devices and password protection. For further information please refer to the Mobile and Remote Working Policy.

7. SUPPLIER'S REMOTE ACCESS TO THE COUNCIL NETWORK

7.1 Partner agencies or 3rd party suppliers must not be given details of how to access the Council's network without permission from IT within a business case. Any changes to supplier's connections must be immediately sent to the IT Service Desk so that access can be updated or ceased. All permissions and access methods must be controlled by IT with assurances from the SIRO.

7.2 Partners or 3rd party suppliers must contact the IT before connecting to the TMBC network and a log of activity must be maintained. Remote access software must be disabled when not in use.

8. OPERATING SYSTEM ACCESS CONTROL

8.1 Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (4) and the Password section (10) must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.
- Displaying a general warning notice that only authorised users are allowed.

8.2 All access to operating systems is via a unique login id that will be audited and can be traced back to each individual user. The login id must not give any indication of the level of access that it provides to the system (e.g. administration rights).

8.3 System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

9. APPLICATION AND INFORMATION ACCESS

9.1 Access within software applications must be restricted using the security features built into the individual product. The manager of the software application is responsible for granting access to the information within the system. The access must:

- Be compliant with the User Access Management section (4) and the Password section (10).
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

10. PASSWORD SECURITY

10.1 *Choosing Passwords*

10.1.1 Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be.

10.1.2 A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

10.2 *Weak and Strong Passwords*

10.2.1 A *weak* password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a

dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

10.2.2 A *strong* password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

10.2.3 Everyone must use strong passwords with a minimum standard of:

- A minimum of seven characters.
- Contain a mix of alpha and numeric, with at least three non-alphabetic characters (i.e. numbers and/or symbols).
- More complex than a single word (such passwords are easier for hackers to crack).
- For further password guidance, click here to visit the IT Service Portal and type 'password' in the search box.

10.3 *Protecting Passwords*

10.3.1 It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different TMBC systems.
- Do not use the same password for systems inside and outside of work.

10.4 *Changing Passwords*

10.4.1 All user-level passwords must be changed at a maximum of every 42 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to the SUM or Information Asset Owner

10.4.2 Users **must not** reuse the same password within 20 password changes

10.5 *System Administration Standards*

10.5.1 The password administration process for individual TMBC systems is well-documented and available to designated individuals (Draft Note.

10.5.2 All TMBC IT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users (i.e. no generic accounts).
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

11. COMPLIANCE

11.1 This TMBC Access Control Policy takes into consideration all applicable statutory, regulatory and contractual security requirements.

11.2 It is the responsibility of Managers to exercise appropriate controls to minimise the risk of unauthorised access and where misuse is suspected to report it via the Information Security Incident Management process

11.3 It is the responsibility of all employees to ensure that they have read and comply with the conditions laid out in this policy.

11.4 Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

11.5 If any user is found to have breached this policy, they may be subject to TMBC disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

11.6 If you do not understand the implications of this policy or how it may apply to you, seek advice from the Risk and Insurance Manager.

12. REFERENCES

12.1 This TMBC Access Control Policy should be read in conjunction with the overall Information Security Policy and related sub-policies.

12.2 The following TMBC policy documents are directly relevant to this policy, and are referenced within this document:

- Mobile and Remote Working Policy.
- Information Security Incident Management Policy.

APPENDIX 11

INCIDENT REPORTING PROCEDURE

1. INTRODUCTION

1.1 Tameside Metropolitan Borough Council (the Council) will ensure that it reacts appropriately to any actual or suspected incidents relating to electronic or paper based information systems within the custody or control of the Council or its contractual third parties.

1.2 This procedure must be applied as soon as Council information or information systems are suspected to be, or are actually affected by an adverse event which is likely to lead to an Information Security Incident (ISI).

1.3 All incidents, irrespective of scale, must be reported using the incident management procedure to allow for lessons to be learned and to improve information handling procedures and the incident response process.

2. DEFINITIONS

2.1 The following terms are used throughout this document and are defined as follows;

Information Security Incident (ISI) is defined as an adverse event that has caused or has the potential to cause damage to the Council's assets, reputation, personnel and/or citizens.

An ISI can occur when there is an actual or potential loss of information or when information is discovered (e.g. USB memory stick/paper files found or handed in).

On some occasions, an ISI will include personal data and will entail a breach of the Data Protection Act.

Examples of Information Security Incidents have been provided at **Appendix 1.**

Personal information: is any personal data as defined by the Data Protection Act 1998. Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of personal information held by it as governed by the Data Protection Act 1998.

Sensitive personal information: is any personal information (as defined above) which consists of details relating to their:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- mental/physical health or condition
- sexual life
- a committed or alleged offence
- details of the proceedings or the sentence of any court

Protected Information is any information which is;

(a) personal/sensitive personal data *or*
(b) confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way

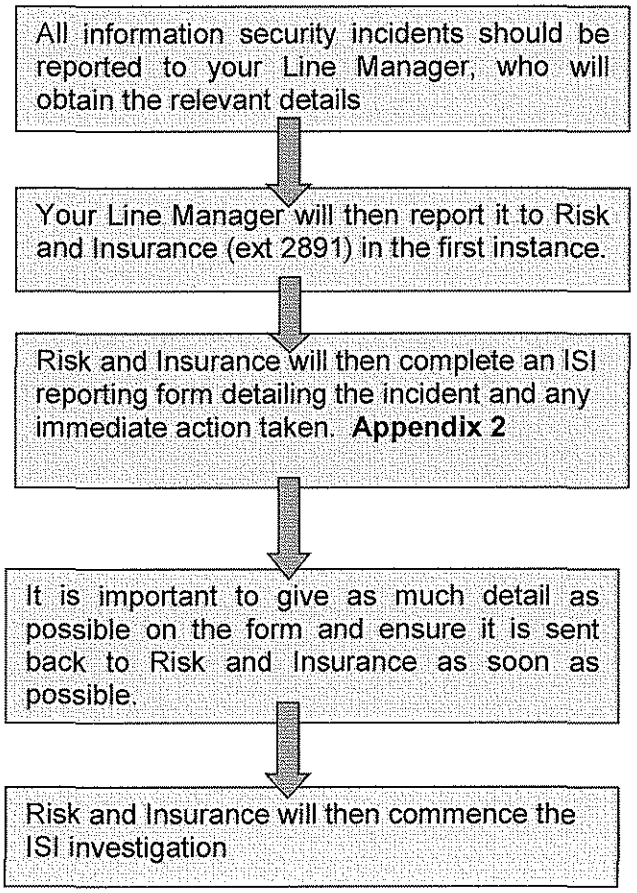
APPENDIX 11

3. ROLES AND RESPONSIBILITIES

3.1 All employees must understand and adopt the use of this procedure and are responsible for safe and secure use of Council information and systems.

3.2 All employees have a duty to report actual or suspected ISI and to fully support an investigation. Failure to report an ISI within 24 hours of discovery could result in a disciplinary action.

4. Reporting an Incident



Note: *If information has been discovered in any format, it is important that you do not do anything with the information unless advised to do so by Risk and Insurance. Report as you would normally through the ISI process outlined above.*

5. INCIDENT INVESTIGATION

5.1 *Initial Response*

5.1.1 Once the ISI form has been completed an evaluation can take place to identify if, there may be a need for immediate action in order to limit the damage from the breach and recover any losses. Action may also be needed to prevent another breach with similar circumstances whilst the investigation is taking place. This may include action taken to:

- prevent any further unauthorised access
- secure any affected buildings (i.e. changing locks, access codes etc.)
- recover any equipment or physical information
- restore lost or damaged data by using backups
- prevent a further breach relating to the same information (e.g. an attempt to use stolen data to access accounts or services)

5.1.2 The Risk and Insurance Manager will determine if any immediate action needs to be taken based on the details provided and will notify the relevant persons.

5.2 ***Investigation Process***

5.2.1 The Risk and Insurance Manager at this stage will commence an investigation. The investigation may involve the following:

- Senior Information Risk Owner (SIRO)
- Data Protection Officer/Data Controller
- Service Director or a representative for the relevant part of the directorate
- Line Manager of person who has made the breach
- Head of Human Resources or a representative
- Head of ICT/ICT Security Officer
- Head of Media, Marketing and Communications or a representative
- Facilities Management
- Caldicott Guardian

5.2.2 Depending on the type and seriousness of the incident, the police may be involved and the employee/s suspended from the work place.

5.2.3 The Risk and Insurance Manager will use the checklist outlined at **Appendix 3** along with any other information required, to investigate the incident and will record any key findings from this point forward.

5.2.4 Once the investigation is completed, a summary of the incident will be presented to Senior Management for evaluation and signing off.

6. EVALUATION

6.1 A consistent approach to dealing with all security incidents must be maintained across the Council and each incident must be evaluated. It is important not only to evaluate the causes of the breach but also the effectiveness of the response to it.

6.2 The evaluation of the ISI will include some of the following questions:

- Had the incident been identified as a risk prior to its occurrence?
- Did the incident occur despite existing measures being in place?
- Were current policies and procedures followed? If not, why not?
- In what way did the current measures prove inadequate?
- How likely is the incident to recur?
- Did the incident involve deliberate or reckless behaviour?

6.3 *Assessment of Ongoing Risk*

6.3.1 Any identified weaknesses or vulnerabilities must be accurately assessed in order to mitigate the ongoing risks to information. In order to make an assessment, the following factors will be considered:

- Type of data involved
- Number of people that could be affected
- Impact on individuals
- Protections in place (e.g. encryption)
- Likelihood of the identified risk
- Possible consequences for the Council's reputation
- Potential risks to public health or safety

7. ACTIONS

7.1 Once the investigation and the evaluation of the incident is concluded, any identified actions will be approved by Senior Management and implemented appropriately throughout the Service involved or if required the whole organisation.

7.2 *Notification*

7.2.1 Depending on the incident there may be legal, contractual or sector specific requirements to notify various parties. Notification may assist in security improvements and implementation, as well as risk mitigation.

7.2.2 The following parties may need to be notified following an ISI:

- ***Information Commissioner's Office (ICO)***
  - Does the incident involve personal data? If so:
  - Does the type and extent of the incident trigger notification?
- ***Individuals***
  - Notification to the data subjects involved maybe required
- ***Other Agencies*** *(not an exhaustive list)*
  - Identity and Passport Service
  - Her Majesty's Revenue and Customs (HMRC)
  - Bank or credit card companies
  - Trade Unions

7.2.3 Notification to any parties will be determined and agreed by Senior Management as part of the evaluation of an incident.

7.3 *Disciplinary Action*

7.3.1 It may be deemed necessary to follow the disciplinary procedure for any employee(s) involved in an ISI.

7.4 *Policy and Procedural Changes*

7.4.1 There may be a need to implement policy and procedural changes as a result of an ISI.

APPENDIX 11

7.5 Employee *Notification and Training*

7.5.2 There may be a requirement to notify employees of policy and procedural changes and to repeat, extend or revise training following an ISI.

APPENDIX 11

Appendix 1

Examples of Information Security Incidents (ISIs)

Examples of Information Security Incidents (ISIs) are listed below. It should be noted that this list is not exhaustive.

- Giving information to someone who should not have access to it - verbally, in writing or electronically
- Computer infected by a Virus or other malware
- Sending a sensitive e-mail to 'all staff' by mistake
- Receiving unsolicited mail of an offensive nature
- Receiving unsolicited mail which requires you to enter personal data
- Hacking attacks which intend to gain information from computers and/or systems using a number of methods (e.g. phishing, password cracking, key logging)
- Changes to information or data or system hardware, firmware, or software characteristics without appropriate authority or the Council's knowledge, instruction, or consent
- Receiving and forwarding chain letters – including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others
- 'Blagging' offences where information is obtained by deceiving the organisation that holds it (including information which could assist in gaining access to council data e.g. a password)
- Use of unapproved or unlicensed software on Council equipment
- Accessing a computer database using someone else's authorisation (e.g. someone else's user id and password)
- Writing down your password and leaving it on display / somewhere easy to find
- Printing or copying confidential information and not storing it correctly or confidentially
- Theft / loss of a hard copy file
- Theft / loss of any Council computer equipment on which information is stored
- Discovery of hard copy information or electronic media on which information may be stored (e.g. disc or USB memory stick)
- Unwanted disruption or denial of service to a system which may cause an adverse affect to the information held within
- Equipment failure that results in the loss of or damage to information
- Unforeseen circumstances such as fire or flood that damages information or areas where information is stored
- Posting inappropriate comments or material online (including on social networks)

APPENDIX 11

Appendix 2

Information Security Incident (ISI) Reporting Form

Directorate	
Service Area	
Line Manager	
Employee Reporting Incident	
Date/Time of Incident	
Type of Data*	

* Examples of data:
- Files/Paperwork containing personal data
- Emails stored on a laptop/PDA
- Data stored on an information system (e.g. Agresso)

Details of incident:	
Briefly describe the circumstances of the incident:	
Give an outline of what the data consists of: (please ensure this includes all the types of data involved)	
Approximately how many people have been affected?	
Has there been any media coverage of the incident?	
Are any other partners involved?	
Immediate action taken:	
Have you taken any action to minimise/mitigate the effect on the data subjects involved? If so please provide brief details:	

Completed By: Date:

APPENDIX 11

Appendix 3

Information Security Incident (ISI) Investigation Checklist

The following questions may be asked during the investigation process.

How was the incident discovered?

What type of data is involved?

- Health or Social Care?
- Financial (e.g. bank details)?
- Personally Identifiable Information (e.g. address, NI number)?

Whose data is involved?

- Service users, patients or customers?
- Councillors?
- Council employees?
- Suppliers or partners?

How many people could be affected by the incident?

What could the information be used for?

What impact has the incident on?

- **Data Subjects:**
  - Physical harm
  - Mental anguish/distress
  - Reputation/embarrassment
  - Financial loss
  - Identity theft
  - Breach/loss of confidence
- **Employees:**
  - Embarrassment
  - Mental anguish on employees involved
  - Interruption of service to clients
  - Loss of confidence in service provision
- **The Council:**
  - Embarrassment/reputational damage
  - Breach/loss of public confidence
  - Press involvement
  - Potential legal action

What immediate action has been taken to recover the information?

Had the incident been identified as a risk prior to its occurrence?

What controls were in place to prevent the incident?

How likely is the incident to occur again?

Are the relevant employees aware of current policies and procedures?

Did the incident involve deliberate or reckless behaviour by an employee?

Please note that this list is not exhaustive. Other questions may be asked depending on the nature of the incident.

APPENDIX 12

SECURE DESK PROCEDURE

1. INTRODUCTION

1.1 A secure desk is essential to mitigate the risks associated with unauthorised access to Tameside Metropolitan Borough Council (the Council) information. Applying a secure desk procedure reduces the threat of a security breach as information is kept out of sight.

1.2 In order to enable employees to work in a more efficient way, the Council is moving towards a shared working environment and there may be a requirement for an employee to work in different locations or for more than one employee to use a desk or a work station. To facilitate such a change in the working environment, a secure desk procedure is essential to ensure that each work space is productive and protected.

1.3 This procedure applies to all information of a personal, confidential or sensitive nature. It also takes into account any information that is accessed, viewed or stored within a shared space (i.e. main office, home or Touch Down Point).

2. DEFINITIONS

2.1 The following terms are used throughout this document and are defined as follows:

Personal information: is any personal data as defined by the Data Protection Act 1998. Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of personal information held by it as governed by the Data Protection Act 1998.

Sensitive personal information: is any personal information (as defined above) which consists of details relating to their:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- mental/physical health or condition
- sexual life
- a committed or alleged offence
- details of the proceedings or the sentence of any court

Protected information is any information which is;

(a) personal/sensitive personal information *or*
(b) confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.

3. ROLES AND RESPONSIBILITIES

3.1 All employees must ensure that their work environment follows the secure desk procedure.

3.2 It is the responsibility of individual services to implement this procedure and monitor work areas.

3.3 It is the responsibility of all individuals to immediately report any actual or suspected breaches in information security by following the Incident Reporting Procedure.

4. SECURE DESK PROCEDURE

4.1 The secure desk procedure is required to ensure that all protected information is held securely at all times. Information identified as protected must not be left out on desks when unattended to prevent information being read by unauthorised parties.

4.2 For periods away from your desk, working papers containing protected information must be placed out of sight and, where necessary, in a locked cupboard or drawer. Information that is not protected (i.e. contains no personal, sensitive or confidential data) may be left tidily on desks.

4.3 At the end of each day, all protected information should be stored in locked cupboards/drawers or within a locked room. Protected information should not be left on view. Computer equipment must be shut down or taken with you.

4.4 Protected information should not be left lying on printers, photocopiers or fax machines, even if they are in a locked room. These should all be checked at the end of the working day and any papers stored securely overnight.

4.5 Whenever you leave your desk and your PC is switched on, you should lock your computer by pressing Ctrl, Alt and Delete and then confirm that you wish to lock your workstation.

4.6 If you are working on protected information and you have a visitor to your desk who does not have a need to know that information, ensure that you lock your screen or ensure that the information is not visible to them to prevent the contents being read. Even the knowledge that a file is held on a person can be considered an information breach.

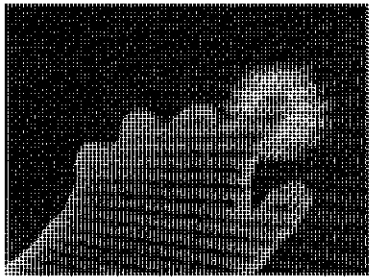
4.7 All waste paper which contains protected information must be disposed of appropriately (i.e. shredded or placed in red bins). Under no circumstances should this type of waste paper be thrown away in normal rubbish or recycling bins. For further information on the secure disposal of information see the Retention and Disposal Guidelines/Schedule.

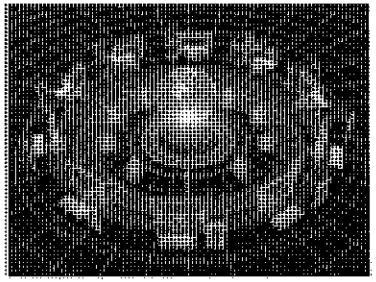
4.8 Protected information should not be stored in boxes and/or folders on top of any furniture (cabinets etc). This is insecure as they can still be accessed.

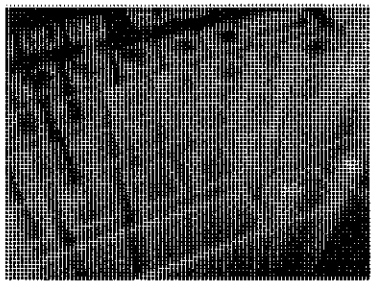
4.9 When using a hot desk or touch down point, you must consider the length of time you may be away from a desk (to attend a meeting, go for lunch, etc.). It is important to think about the security of your surroundings and secure any protected information where necessary.

Tameside MBC

Personal Device Policy







Tameside Metropolitan Borough

APPENDIX 13

Contents

Tameside Metropolitan Borough

Document Control

Name	Version	Description	Date
Julie Hayes	.01	Draft	2 January 2013
Risk and Audit	.02	Draft	3 January 2013
Organisational Development	.03	Draft	4 January 2013
Paul Turner	.04	Draft	8 January 2013
IRMG	.04	Draft	9 January 2013
	1	1st Published version	13 March 2013
	1.1	Clarification of some points	21 March 2013

1 Introduction

1.1 The Council wants to encourage its staff to work as efficiently as possible. It provides staff with the essential technology they need to do their job. However it cannot provide all employees with every type of device which might conceivably be useful to them in their work.

1.2 The Council recognises that many of its employees have purchased their own electronic devices for their personal use and that some staff are willing to use their device for work purposes in order to help them do their job.

1.3 The Council wants to allow its employees this facility as far as possible. However, the Council is subject to legal rules and must ensure that access to its data is safeguarded. This policy has been designed to allow as much flexibility as possible whilst meeting the operational needs of the Council.

1.4 The main risks associated with this are the potential loss or exposure of personal data. The Council is under a legal duty to take appropriate organisational and technical safeguards to ensure the security of personal data. Breach of data security means that the Information Commissioner can fine the Council up to £500,000 and fine individual employees up to £50,000.

1.5 Managers are directly responsible for disseminating and implementing this policy.

1.6 All references to Council data refer to data for which the Council is data controller – this is not limited to personal data but also includes data which is not known to the public.

1.7 In the event of any conflict the ICT Security Policy will take precedence except where it relates to the connection of personal devices to the Council's network.

2 When can I use my personal device to access Council Data?

2.1 You can use your own equipment to access the Council's systems and data from the Council's network if you do so in accordance with this policy.

2.2 This policy only allows access to Council systems on personal devices in one of the following ways:

(a) Via a website made available to you for that purpose (for example Outlook Web Application - OWA).

(b) Via Netilla (if you are an authorised Netilla user and your device supports this).

(c) In a way which is managed by the Council's approved mobile device management software (currently Mobile Iron).

To be clear this means that Active Sync cannot be used on personal devices except as covered in (c) above.

2.2 The use of your own equipment to access council networks is prohibited except in accordance with this policy.

3 Use of personal devices

3.1 You must not download documents containing personal data or other material to your device.

3.2 You must regularly check your device to ensure that no files have been accidentally downloaded and stored on the device (eg by accidentally downloading an attachment to an email). Any such file found must be deleted immediately. Unless you are sure that you do not have data on your device you should protect access to your device using a pass code and, where possible, encrypting that device.

3.3 In particular you must check the device before allowing someone else to use it or before you dispose of the device to make sure that nothing has been accidentally downloaded onto the device.

3.4 Whenever accessing council data you must ensure that you comply with the provisions of this policy as well as the ICT Security Policy, Acceptable Use Guidelines, the Data Protection Act 1998 and all Information Risk Management policies, which can all be found on the intranet. By using a personal device to access the Council's systems and data, an individual is accepting responsibility for the safeguarding of data viewed on that device and will be held accountable for any incidents which compromise the safety of that data. Failure to adhere to these policies may lead to disciplinary action being taken and for more serious cases, where individuals have not followed guidance and policies, legal action. In addition it should be noted that an individual fine can be imposed by the Information Commissioner's Office (ICO) in the event that the personal device is purposefully used to obtain information for an individual's own financial or personal benefit.

3.5 You must not connect your personal device to the Council's private wifi network (although you are permitted to use the free public wifi hotspots located in some Council buildings).

3.6 Individuals who wish to take advantage of this policy do so at their own expense. The Council will not reimburse individuals for any support costs they incur nor will it reimburse the cost of supplying data to the device or for any damage to the device caused by the installation or removal of mobile device management software.

3.7 Individuals must notify the Council IMMEDIATELY if any of the following occur,

- a device that has been set up to access the Council's systems is lost,
- the device has been damaged/has developed a fault,
- if the device is handed – temporarily or permanently to a third party for repair or other reason.

In all cases the facility to access the Council's systems and data will be removed.

4 Use of personal devices with Mobile Device Management (MDM) Software

4.1 The following applies only where method 2(c) is used to access the Council's systems and data.

4.2 Mobile device management software will only be available where

(a) A service (or an individual employee) is prepared to pay the annual cost of the licence for that software.

(b) The employee has a device covered by this policy as shown in Appendix 1.

(c) The individual signs a personal device agreement (shown in Appendix 2).

(d) The service agrees that this facility is appropriate for the employee concerned. For example, if an individual handles personal information on behalf of other organisations, steps should be taken to check that the Council is not breaching any information sharing protocols or data exchange agreements. If an individual handles very sensitive personal data then the service must ensure that the protection offered by the software is adequate to protect the data. Section 5.3 of this policy is also relevant to this assessment.

4.3 Once the fee has been paid, the employee will be set up in the system and a notification will be sent to confirm this has been done.

4.4 The employee is responsible for downloading and installing the mobile device management software and must ensure that:

(a) Council data cannot be accessed by friends and family.

(b) Council data is only stored on the device if that data is controlled by the mobile device management software.

(c) Council data is not transferred from the device to any other device or storage medium.

(d) Any instructions given in relation to their device are followed. This could include a requirement to:

- Update software or operating system.
- Protect the device with a passcode lock.
- Install software.
- Delete software.
- Configure the personal device in a particular way.

(e) Council data is deleted if the Employee leaves the Council or if the Council requires.

4.5 The Council will not provide support or training in the use of your device except about Mobile Device Management software.

4.6 The Council remains the owner of all council data on the device. It has the legal duty to control that data. For that reason employees who participate in this agreement give the Council some control over the device. They are giving the Council the right to:

(a) Delete Council data from the device or lock the device or that data.

(b) Scrutinise the employee's device.

(c) Require the employee to allow the device to be physically inspected.

(d) Collect systems data about the personal device on an ongoing basis, which will be stored in the Mobile Device Management (MDM) system. The data will only be used by the Council for necessary administration, business purposes and to support the investigation of misuse, fraud, criminal activity or data loss if necessary. Data will include but is not limited to

- Telephone number
- International Mobile Equipment (IMEI) number
- Make and Model
- Operating System and version
- Configuration
- Applications installed

In addition the Mobile Device Management (MDM) system will collect data in relation, but not limited to

- Device location
- Council systems and data accessed by the device

(e) Collect data about applications an individual has installed on their device. If the Council considers that an application may compromise the Council's systems and data it will delete council data from the device and suspend access to council data.

(f) Require the employee to attend training as necessary for the Mobile Device Management (MDM) software or in relation to Data Protection/Information Management.

4.7 ICT Services may remove the facilities to access the Council's systems and data, remote wipe and/or initiate a remote lock of the device if it considers it appropriate to do so. It may not be possible to give advance warning or seek permission on an individual basis.

5 Costs of use of personal devices with MDM Software

5.1 The following costs apply where method 2(c) is used.

5.2 The cost of the infrastructure to set up the Mobile Device Management (MDM) system will be funded by ICT Services.

5.3 The MDM software annual licence fee for each individual must be funded by that individual's service. Managers must therefore balance the benefits of the individual using their personal device with the cost of the licence to manage and protect the Council's systems and data on that device. This may be attractive where the individual was previously allocated a Council owned Blackberry. Licences may be transferred to another individual. If the individual is part of another service that service will take on the on-going annual commitment but there will be no in year adjustment.

5.4 The individual granted permission to use their own device to access the Council's systems and data must ensure they understand their own contract and data/call allowances as they will be liable for all costs (except those identified in 5.3) incurred when using the device, including but not limited to, data costs (including roaming costs), call charges (even when used for business calls), support from their provider, repair and insurance costs.

5.5 The Council will not reimburse individuals for business calls made. Where an individual needs to make a large number of work-related calls it is likely that a Council issued device will be more appropriate.

5.6 The Council will not accept liability for damage, theft or loss of an individual's personal device, no matter how caused. This applies even in the event of a device being damaged whilst being used to access Council data.

5.7 The Council will not accept liability for damage, theft or loss of an individual's personal data including music and applications, no matter how caused. This applies even in the event of a device being damaged whilst being used to access Council data.

5.8 The Council may under certain circumstances reimburse individuals for additional charges in a disaster recovery situation emergency (but prior approval is needed for this).

Appendix 1 – Approved and Excluded Devices

Excluded Devices

Please note that list is subject to change without notice should a device become a security risk to the Council's systems or data.

- Devices that have been 'Jailbroken', 'hacked', 'rooted' or in any way tampered with.
- Devices with the following operating systems
    - IOS 3 or earlier
    - Symbian 3rd Edition, base, FP1, FP2, 5th generation
    - WebOS
    - Windows Mobile 5

Approved Devices

Please note that list is subject to change without notice should a device become a security risk to the Council's systems or data.

- Devices with the following operating systems
    - Android 2.2 and later
    - Blackberry 4.2.1 and later
    - IOS4.x+ MDM
    - Windows Mobile 6
    - Windows phone 7.x
- Any personal laptop, computer or other device using methods outlined in Section 2 (a) and (b) of this Policy.

Appendix 2 – Personal Device Agreement

For use where an employee is to be granted permission to access the Council's systems and data using their personal device managed by the Council's approved mobile device management software (currently Mobile Iron).

Name	
Service	
Device	
Authorised by	
Location of documented assessment of appropriateness by manager.	
Date effective from	

In consideration of the Council agreeing to allow me to access its data on my personal device I agree that :-

1. I will comply in full with the requirements of the Personal Device Policy (as available on the Council's intranet from time to time).
2. The Council may take any action in relation to my device and collect information about my device in accordance with the Personal Device Policy (as available on the Council's intranet from time to time).
3. I will comply with all instructions given to me under the Personal Device Policy (as available on the Council's intranet from time to time).
4. I understand my responsibility for safeguarding all council data.
5. I understand that the Council and I can end this agreement at any time but that if the agreement is ended then the Council will have permission to delete its data and software from my device and that if necessary I will need to present the device to the Council at my own expense and help staff ensure that Council data has been deleted from the device.

I note that if I do not comply with the policy or break this agreement then I may be subject to disciplinary action.

Signed.....
Dated.....

APPENDIX 14

Information Security – Golden Rules

Information is a valuable asset. The Council has a duty and responsibility to protect it. This responsibility is placed on the Council by the Data Protection Act 1998 monitored and regulated by the Information Commissioner's Office.

The Information Commissioner has powers to impose monetary penalty notices for up to £500,000 for breaches of the Data Protection Act, along with having the authority to carry out assessments of organisations to ensure their processes follow good practice. The key guidance document that the Council would be measured against is the Local Public Services Data Handling Guidelines produced in August 2012 by the Public Services Network. The Council wants to comply with these guidelines to ensure good practice is being followed. The Council needs to ensure that everyone uses and manages information assets and information systems in an effective, efficient, and ethical manner.

The objective is to protect the Council's information assets from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities. The Council is committed to protecting information through preserving:

Confidentiality - Protecting information from unauthorised access, use and disclosure from unauthorised individuals, entities or processes.

Integrity - Safeguarding the accuracy and completeness of information assets. This may include the ability to prove that an action or event has taken place so that it cannot be repudiated later.

Availability - Being accessible and useable on demand by an authorised individual, entity or process.

It is essential that you understand your data protection and security obligations and that every day business practice helps foster an organisation wide security-aware culture embracing good data handling behaviours.

These Golden Rules aim to help you:

- safeguard the Council's valuable information assets, systems and equipment
- use information assets responsibly within the framework of the law
- make sure you understand the corporate policies with which you must comply
- signpost the mandatory corporate on-line training you must undertake

All employees must comply with the minimum corporate security standards set out in these rules which are based on the Council's Information Governance Framework of policies, procedures, standards and guidance and also ensure you follow any localised business specific data handling requirements.

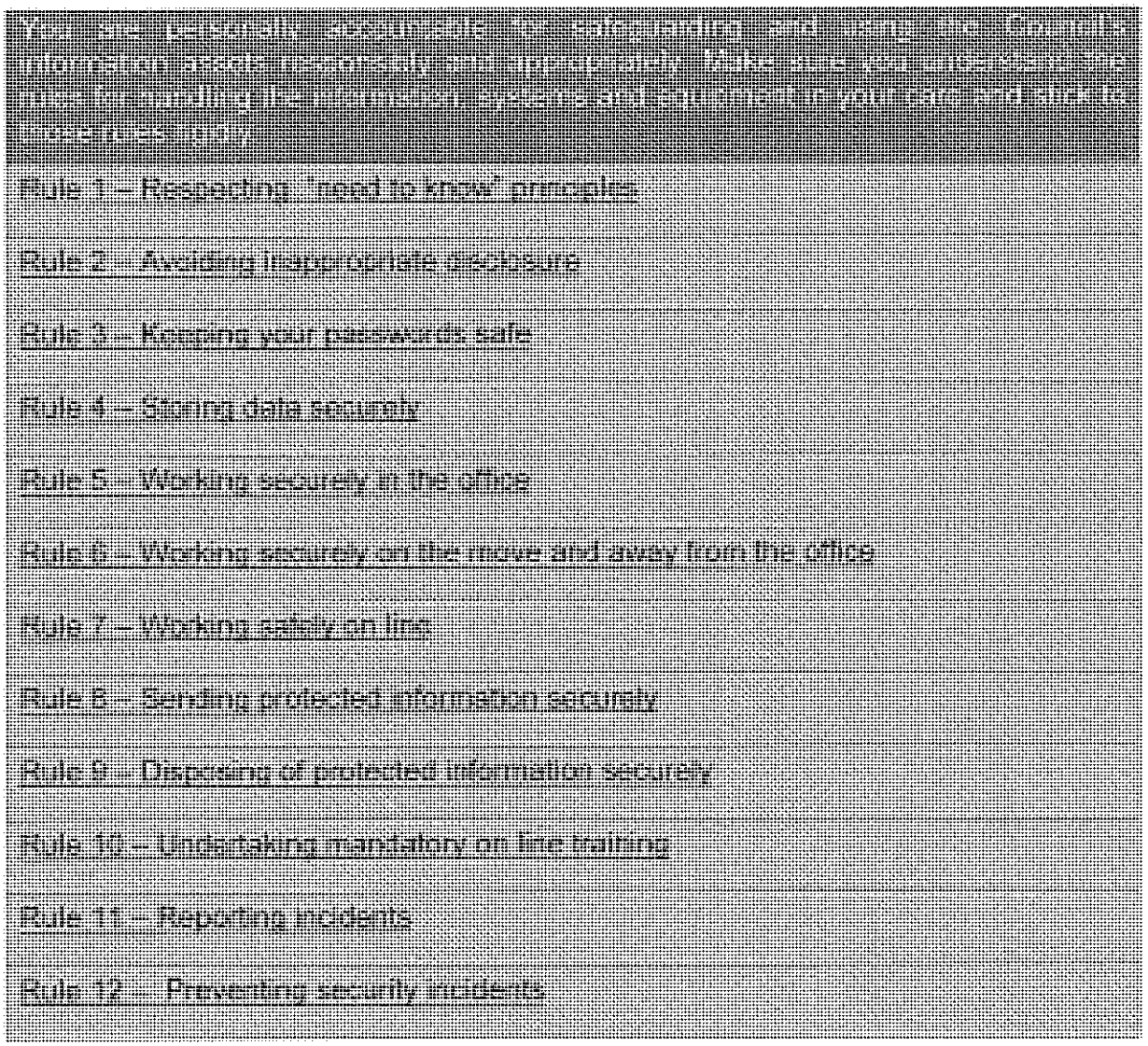
Protected Information is any information which is:-

- personal/sensitive personal information; or
- confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way

Personal information: is any personal data as defined by the Data Protection Act 1998. Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of personal information held by it as governed by the Data Protection Act.

Sensitive personal information: is any personal information (as defined above) which consists of details relating to their:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- mental/physical health or condition
- sexual life
- a committed or alleged offence
- details of the proceedings or the sentence of any court



Rule 1: Respecting "need to know" principles

- Only access protected information if it is part of your job and you have a legitimate business need to know
- Never access protected information for personal interest or gain
- If you need protected information 'owned' by another business area to do your job, make sure you are authorised to ask for it, you only ask for the minimum necessary for the required purpose and, you are clear why you are entitled to it

Rule 2: Avoid inappropriate disclosure

- Before disclosing protected information to an external third party always ask yourself *"is this request legitimate?"* and verify that the requester is who they say they are.
- Always make certain you have the legal authority, including the legal power to disclose the information.
- Check whether the purpose could be satisfied with anonymised rather than protected information.
- Keep a documented audit trail of all ad hoc disclosures.
- If you are unsure of the rules, check with your manager, Legal Services or the Risk and Insurance Manager.

Rule 3: Keeping your passwords safe

- Protect passwords at all times.
- This applies to all passwords enabling access to data and to the Council's network, business systems, email and the internet.
- Avoid writing your password down and if you have to, don't leave it in obvious places such as under your keyboard, next to your monitor or other easily searchable places.
- Ensure that your password is sufficiently complex that you can remember it but it cannot easily be guessed by others.
- Immediately change your password if you suspect it may have been compromised.
- Please refer to the ICT Service Portal for Password Guidance. Click here and type 'password' in the search box.

Rule 4: Entering & storing data securely

- Enter data accurately and completely.
- Physical files containing protected information must be locked away securely.
- Always save electronic files on the Council's network drives and do not keep the information on your local computer hard drive.
- Remember the secure network is automatically backed up and remains available even if your computer fails.
- If you are working away from the office, access to view or amend data should be via a secure remote connection to Tameside's network.
- If this is not possible and permission is granted to create or store protected information on encrypted portable devices or removable media, this must be the minimum necessary for the approved business purpose.
- The authorised user is responsible for ensuring that unique data held on encrypted devices is regularly backed up to the Council's secure network.
- Information assets must be managed in accordance with the retention and disposal guidelines. Once no longer required for legal, regulatory or business purposes, information should be securely destroyed in line with the retention and disposal schedules for your service area.

Rule 5: Work securely in the office

- Never leave protected information or other valuable assets out on your desk when you are not around.
- Remove documents from printers and copiers as they are produced to avoid them being picked up by mistake, or read by someone else.
- When sending information by post check that you have only included the correct documents, especially if collected from shared printers/copiers.
- Lock your work station, log off at the end of the day and switch off your screen.

- Lock windows, offices and conference rooms containing physical records and computer equipment whenever the area is unoccupied.
- Wear your pass when you are in Tameside buildings, remove it and keep it safe when you leave.
- Challenge anybody you see in your building who is not wearing an appropriate security pass.

Rule 6: Work securely on the move and away from the office

- If you are authorised to carry protected information in paper files and/or on encrypted devices beyond your secure workplace keep your laptop, Blackberry, and official papers with you at all times and take reasonable precautions based on the environment you are in.
- Ensure that you:
  - comply with local physical file tracking procedures;
  - make sure your laptop is protected with encryption software;
  - avoid *"shoulder surfers"* in public places viewing your screen or confidential business conversations being overheard;
  - do not leave protected information or equipment in an unattended vehicle; and
  - limit the risk of valuable information or equipment being lost or stolen (i.e. by not taking council resources to places where they are at risk of being stolen).
- Always ask yourself the question *"Do I really need to take protected information out of the office?"* The best way to prevent theft or accidental data loss is to leave it safely on Council premises.
- Only take the minimum necessary paper records with you (rather than the whole file).
- Do not let unauthorised people, including family members, use or view valuable council resources.
- If you have encrypted equipment and protected information in physical files overnight in your home, reduce the risk by ensuring that the unencrypted physical files are locked away separately.

Rule 7: Working safely on line

- Make sure you understand the Council's internet and email policies.
- Never open an email from sources you do not know and trust.
- Always report any unusual email messages or suspicious attachments or links especially in unsolicited emails.
- Never use non-Tameside email accounts to send or receive protected information.
- Follow the IT security policy.

Rule 8: Sending protected information securely

- Make sure you know what protective marking applies and stick to the rules for that level of protection whenever you have to send protected information, especially outside the Council.
- Be diligent when sending letters, addressing envelopes, choosing fax numbers and email addresses to prevent errors and misdirection.
- Try to limit the harm which might be caused if something goes wrong by thinking about whether you need to play back sensitive details (i.e. identifiers or bank account numbers the recipient has previously supplied) and send only what you absolutely need to send and no more.
- Do not send protected information by external email ***UNLESS***:
  - You have a GCSX account and are sending it securely to another GCSX mail account (or any of the other secure government networks); ***or***
  - You are sending it in an attachment, using strong password protection and encryption software.

- If you are sending protected information by internal email, within the Council's secure network, always check you have addressed the email correctly to avoid sending it to the wrong person.
- Do not send protected information to a generic mail address unless appropriate and you actually know the mail address relates only to a Tameside internal mail account.
- Only transport protected information on removable media (cameras, DVDs, memory sticks etc) if you are using Council supplied devices and obtain assurance that the device or the information stored on it, is encrypted to recognised industry standards.

Rule 9: Disposing of protected information securely

All resources containing protected information must be disposed of securely. This applies to protected information held in various formats including:

- paper records (e.g. printed notes, assessments, correspondence or reports).
- electronically stored on encrypted laptops and other portable devices.
- stored on approved removable media, for example writable CDs, writable DVDs, external hard drives, audio and video tapes.

Portable laptops that are no longer required must be returned to ICT enabling the hard drive to be permanently erased with specialist software before disposal or recycling to another business area.

Removable media devices that are no longer required, or have become damaged, must be returned to the ICT Service for secure disposal.

Confidential paper waste must be kept separate from ordinary paper waste and protected from accidental loss, damage or unauthorised access until its final removal/disposal. Follow the minimum standards in the Council's corporate policy for disposing of waste, as supplemented by locally agreed business operating procedures.

Particular care must be exercised during office relocations and moves to ensure that all confidential paper waste and non-required ICT equipment is disposed of properly.

Rule 10: Training

On line Information Governance training is currently under review and will be available shortly.

Undertake the Data Protection E-Learning tutorial http://dp.tameside.gov.uk/.

A Data Protection video produced by the ICO is available on the Staff Portal and all employees should watch it.

Further guidance is available on the Staff Portal under Data Protection and Information Governance at:-
http://intranet2.tameside.gov.uk/chiefexec/hr/datapro3.htm
http://intranet2.tameside.gov.uk/chiefexec/treasurer/inforisk.htm

Rule 11: Reporting Incidents

You must always report actual or suspected security violations, problems or vulnerabilities to the ICT Security Officer (Ext. 2773) as soon as possible.

If the incident or near miss, involves the loss, theft or unauthorised disclosure of protected information it must be reported to the Data Protection Officer via the form on the Data Protection

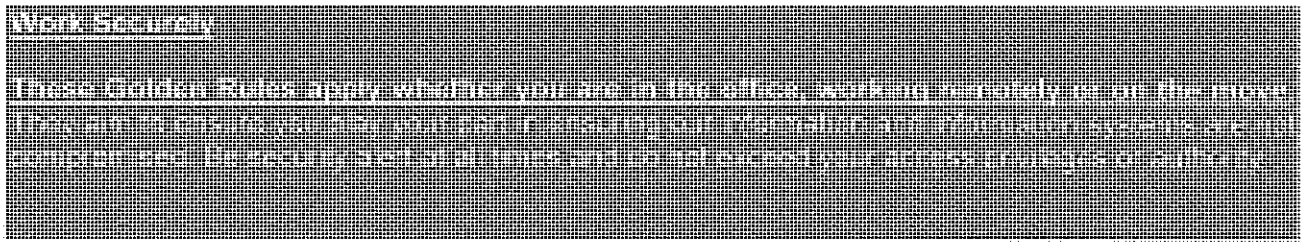
pages on the Staff Portal, an appropriate senior manager as well as the Risk and Insurance Manager - http://intranet2.tameside.gov.uk/chiefexec/hr/datapro3.htm.

Delaying reporting an incident makes it more difficult to solve the problem. Report it straight away so your manager, ICT, Legal Services and Risk Management are able to act quickly and get any expert advice they may need.

Rule 12 – Preventing security incidents

Remember good data security is in your interest too.

Security breaches caused by deliberate, negligent or reckless behaviour could result in dismissal and even give rise to personal fines (up to £50,000) and criminal offences. Make sure you observe the Council's confidentiality, data protection and information governance rules. This will help avoid misuse, unauthorised disclosure, modification, loss or theft of protected information assets which can harm individuals, commercial/partner organisations and/or the reputation of the Council.



APPENDIX 15

INFORMATION GOVERNANCE CHECKLIST

To ensure the security and confidentiality of the Council's information and the security of its assets and premises, Managers/Supervisors have been provided with the following checklist to enable you to identify the areas you should be considering on a regular basis. Any queries about the below can be clarified with the Risk and Insurance Manager Ext 2891, ICT Security Officer Ext 2773 or Legal Services.

DIRECTORATE/SEVICE UNIT:

1. Secure Desk Policy			
Action	**Resource**	**Self Assessment**	**Actions**
Make sure staff know that they must secure paper files and loose papers when left unattended	Secure Desk Policy		
Make sure that staff know that they need to ensure that printed documents are not left uncollected on printers and fax machines	Secure Desk Policy, Paper Records & Secure Handling Guidelines, Golden Rules		
Make sure that staff know how to lock their computer when left unattended and that they do so	Secure Desk Policy, System Security		
Make sure staff know that documents and papers must be stored securely when they finish work	Secure Desk Policy, Golden Rules		
Establish if a process of authorisation for allowing confidential information to leave the premises is needed and put in place.			

2. Retention and Disposal Guidance			
Action	**Resource**	**Self Assessment**	**Actions**
Make sure that staff know how to dispose of removable media containing personal or sensitive information.	Disposal of Devices		
Make sure that the document retention guidelines have been disseminated and that staff are aware of how long documents/information should be retained for	Retention and Disposal Guidance		
Ensure that disposal records are kept in	Retention and Disposal		

accordance with the guidance issued	Guidance		
Make sure staff know how to dispose of documents securely and that Blue Iron Mountain Confidential bins are available where needed.	Retention and Disposal Guidance		

3. Information Access Procedure			
Action	**Resource**	**Self Assessment**	**Actions**
Review access that staff have to systems and ensure they only have the access needed to perform their role	Access and Security Protocol		
Ensure that a process is in place to ensure that when a member of staff moves/leaves their systems/buildings access is terminated promptly	Access and Security Protocol Leavers & Movers Checklist		
Ensure that staff do not access information for personal interest or gain.	Golden Rules		

4. Removable Media			
Action	**Resource**	**Self Assessment**	**Actions**
Ensure that your staff are aware of their responsibilities under the Data Protection Act	Intranet Data Protection Page, Data Protection Tutorial		
Ensure that staff know how and where they are supposed to report a breach	Contact the Data Protection Officer		
Make sure that unencrypted memory sticks that are no longer able to be used are dealt with as per the guidance on the intranet	Disposal of Devices		

5. Information Sharing Protocol			
Action	**Resource**	**Self Assessment**	**Actions**
Ensure that staff know what information sharing protocols are in place	Information Sharing Protocol		
Ensure that staff are aware if they are able to share information lawfully	Information Sharing Protocol, Golden Rules		
Ensure that staff are aware of the implications of fair processing including the sharing process in a Privacy Notice	Information Sharing Protocol, Data Protection Principle 1, Data Protection Principle 2,		

	Privacy Notice Code of Practice		
Ensure that staff know how to assess if data requested via an FOI is appropriate to release	FOI E Learning, FOI Intranet Page, Information Sharing Protocol		
Ensure staff are aware how to share information securely. Check they know how to send an encrypted attachment.	Self Service Portal 7 Zip, Restrictions on Removable Media, Data Loss Prevention		
Ensure that staff understand the importance of checking the contents of letters are appropriate before sending them and that only the relevant papers are included in the envelope and sent to the correct address.	ICO Fines		
Are encouraged not to use fax machines for the sharing of information, unless it is the only way? If there is no other option are they aware of the safety precautions that must be taken?	ICO You Tube Video, Golden Rules		

6. ICT Security Policy & Acceptable Use Action	Resource	Self Assessment	Actions
Check the understanding of staff in relation to the ICT Security Policy and Acceptable Use Guidelines.	ICT Security Policy		
Check that staff encrypt the content of emails that contain personal or sensitive information	Self Service Portal 7 Zip, ICT Security Policy		
Check that staff are aware of their responsibilities regarding social media	Social Media Use, Information Governance Conduct Policy, Live Wire March 2012 Page 10		
Are you and your staff aware of your responsibilities when using the Council's IT and email systems?	IT Security Policy, Legal Position, Information Governance Conduct Policy, ICT Security Policy, Data Protection Principle 7		
Check that staff understand the importance of ensuring that email recipients are checked as being correct before an email is sent	ICT Security Policy		

APPENDIX 15

7. Mobile and Remote Working			
Action	Resource	Self Assessment	Actions
Check that staff understand the importance of being vigilant when reading reports or using laptops in a public place for example being aware of the potential risk of 'shoulder surfers' and conversations being overheard.	Mobile & Remote Working Protocol, Golden Rules		
Make sure that staff that deal with confidential and sensitive data are only using mobiles devices approved and secure for accessing the council's network and information	BOYD Policy, ICT Security Policy, Information Governance Conduct Policy		
Ensure that staff are aware that laptops/information should be kept secure when taken off site and kept out of site when not in use.	Mobile & Remote Working Protocol		

APPENDIX 16

INFORMATION SHARING AND PROTOCOL

1. INTRODUCTION

1.1 Information sharing is essential in order to deliver better, more efficient public services. The sharing or transfer of Tameside Metropolitan Borough Council (the Council) information must comply with all legal and regulatory requirements.

1.2 The Information Sharing Protocol is the overarching document that outlines the standards of expected conduct and applies to all sharing of information. Information Sharing or Processing Agreements will govern specific exchanges of information and will specify what information is to be shared, how it will be shared and to for what purpose the information is required.

1.3 This protocol covers the main types of information sharing;

- **Systematic**, routine information sharing where the same information sets are shared between departments/organisations for an established purpose;
- Exceptional, **one-off** decisions to share information for any range of purposes; and
- Information shared with the public.

1.4 The considerations and security around the sharing of information applies equally to paper and electronic records. All procedures around requests, exchange and retention applies to all information, irrespective of medium.

2. DEFINITIONS

2.1 The following definitions are referenced throughout this document and are defined as follows:

Personal information: is any personal data as defined by the Data Protection Act 1998. Broadly this is information about any living individual, who could be identified from the information or any other information that is in the possession of the Council. The Council is legally responsible for the storage, protection and use of personal information held by it as governed by the Data Protection Act.

Sensitive personal information: is any personal information (as defined above) which consists of details relating to their:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- mental/physical health or condition ;
- sexual life;
- a committed or alleged offence; and
- details of the proceedings or the sentence of any court.

Protected Information is any information which is;

(a) personal/sensitive personal information *or*
(b) confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way

Information Sharing: The disclosure of information from one or more organisation to a third party organisation or organisations, or the sharing of information between different parts of an organisation.

Data Controller: Any legal entity, whether an organisation or individual who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal information are, or are to be processed (e.g. Tameside Metropolitan Borough Council, John Smith and Co., Jones Carpets Ltd, etc.).

Data Processer: Any organisation or individual (other than an employee of the data controller), who processes personal data on behalf of the data controller. There is a higher duty of care upon data controllers when a data processor processes information on their behalf.

3. ROLES AND RESPONSIBILITIES

3.1 All employees have a responsibility to ensure information can be shared legally and professionally and must be aware of any relevant legislation when disclosing information. Employees must not disclose any information that is not in the proper course of their duties and information must never be given to those who are not entitled to it.

3.2 Routine information sharing must be supported by an Information Sharing/Processing Agreement. It is the responsibility of service areas to create, review and monitor agreements.

3.3 Where information is shared between a data controller (e.g. the Council) and a data processor (e.g. a contractor), the use and security of the information remains the responsibility of the data controller.

4. DECIDING TO SHARE

4.1 Factors to Consider

4.1.1 The decision to share or not to share information should be based on an assessment of the likely benefits and potential risks of sharing the information and should take into consideration any legal, ethical and professional obligations. The following factors should be carefully considered;

- What information needs to be shared
- What will it achieve or why it is being shared
- Who the information is to be shared with
- Whether consent is needed to share
- When/how it should be shared
- How to check the sharing is achieving its objectives
- What risks does the sharing pose
- Whether the sharing is covered in the Councils existing notification with the ICO (see the Data Protection Register). The Council's registration number is Z5861307.

4.2 Conditions for Sharing

4.2.1 When deciding to share information, it is important to determine whether it is part of a systematic sharing agreement or if it is a one-off decision. All Information sharing should be assessed using the Information Sharing Checklists (Appendix 2) and must be supported by an Information Sharing/Processing Agreement and a Privacy Impact Assessment should have been undertaken.

4.2.2 One-off requests to share information must be considered on a case by case basis. In an emergency situation, for example, there may not be set procedures for information sharing and a local decision may have to be made. It is beneficial for service areas to be aware of

any relevant legislation, professional guidance or ethical rules that are likely to govern a decision in these circumstances.

4.2.3 For one-off requests, any decision to share must be recorded within an Information Sharing / Processing Agreement, decisions not to share should be recorded on an **Information Sharing Decision Form**. It is good practice to document the reasons for decisions made in case there is ever a challenge to a decision, for example in the form of a claim for compensation in the courts or a complaint to the Information Commissioners Office (ICO).

4.2.4 It may not always be possible to prepare a sharing or processing agreement in an emergency situation; however a record (see Information Sharing Decision form) should be made as soon as possible detailing the circumstances, what information was shared and explaining why the disclosure took place, followed by the completion of an appropriate agreement.

5. FAIRNESS AND TRANSPARENCY

5.1 Telling Individuals about Information Sharing

5.1.1 The Data Protection Act does not specify about how to tell individuals about information sharing. In some cases it is enough to have information available so people can access it if they want to. This approach is acceptable where the information sharing is something people are likely to expect or be aware of already, and to which people are unlikely to object.

5.1.2 In other cases it is good practice to communicate with individuals more actively. This is a legal obligation where a failure to do so would result in unfairness to the individual. To 'communicate actively', positive action must be taken to provide a privacy notice, for example by sending a letter, reading out a script, distributing an email/newsletter, or placing a notice in relevant media.

5.1.3 A good way to decide whether to communicate actively is to try to anticipate whether the individual would expect their personal information to be shared or would object if they knew about it. The need to communicate actively is strongest where:

- you are sharing sensitive personal information;
- the information sharing is likely to be unexpected or objectionable;
- sharing the information (or not sharing it) will have a significant effect on the individual;
- the sharing is particularly widespread, involving organisations individuals might not expect; and
- the sharing is being carried out for a range of different purposes.

5.2 Fair Processing and Privacy Notices

5.2.1 In all cases of information sharing, individuals should be informed that this is happening, or will happen. Generally, individuals should be told about the uses of their information at the point it is first collected. This would be in the form of a privacy notice.

5.2.2 A privacy notice, formally known as a Fair Processing Notice, is a written or oral statement. A privacy notice should be genuinely informative and should help individuals to understand how you will use their information and what the consequences of this are for them. As a minimum, a privacy notice should tell people who you are, what you are going to do with their information, who it will be shared with and why. Some examples of privacy notices are available in Appendix 3.

5.2.3 In some cases a single privacy notice is enough to inform the public of all the information sharing that you carry out. This might be the case where personal information is being shared with a number of organisations for one activity or reason (e.g. marketing purposes). However, if there are a number of information sharing activities, it is good practice to provide information about each one separately. This will allow you to give much more tailored information, and to target it at the individuals affected by the particular sharing. There is a danger that individuals affected by information sharing will not be able to find the specific information they need if only one all encompassing privacy notice is produced.

5.2.4 Furthermore, information sharing arrangements can change over time. It is good practice to regularly review your privacy notice so that it continues to accurately reflect the information sharing activities you are involved in. Any significant changes to your privacy notice need to be publicised appropriately which primarily depends on the impact of the changes on individuals.

5.3 Sharing Without the Individuals Knowledge

5.3.1 Under the Data Protection Act, the general rule is that individuals should be aware that personal information about them has been or is going to be shared, even if their consent for the sharing is not needed. However, in certain circumstances the Act allows for personal information to be shared without the individual even knowing about it.

5.3.2 You can share without an individual's knowledge in cases where, for example, personal information is processed for:

- the prevention or detection of crime;
- the apprehension or prosecution of offenders; and
- the assessment or collection of tax or duty.

5.3.3 An organisation sharing personal information for one of these purposes is exempt from the fairness requirements of the Data Protection Act, but only to the extent that applying these provisions would be likely to prejudice the crime and taxation purposes. For example, the police might ask an organisation to give them information about an ex-employee who they suspect of being involved in a serious assault. If informing the ex-employee that they have given the police this information would tip the individual off and be likely to prejudice the investigation, then the organisation could rely on the exemption and wouldn't have to tell the individual about the disclosure of information. It is good practice to tell the individual as soon as you can that information about them has been shared but this may not always be possible.

Full details of the exemptions are explained by the ICO.

5.4 Consent

5.4.1 Consent is a key aspect of sharing information about individuals and is one of the conditions the Data Protection Act sets out when processing sensitive personal information. Consent can take various forms, but in all cases should be;

Informed: The person giving consent must fully understand why information needs to be shared, what will be shared, who will see their information, the purpose it will serve and the implications of sharing it.

Explicit: The person giving explicit consent must express an agreement to their information being shared for the purpose(s) explained to them. This can be expressed either verbally or in writing.

5.4.2 In seeking consent to disclose personal information, the individual concerned should be made fully aware of the nature of the information sharing. However, there may be circumstances when it is lawful to disclose personal information about an individual without their consent. For example, it may be inappropriate to seek it (e.g. if there is a statutory duty to share information) or there may be an exemption to the Data Protection Act that allows for information to be shared without the consent of an individual (e.g. public interest requires the disclosure of personal information).

5.4.3 Records of consent (or refused consent if appropriate) must be clearly recorded to ensure that any sharing of personal information is compliant with the Data Protection Act. Any decision to share information without consent must also be documented.

6. INDIVIDUAL'S RIGHTS

6.1 Access to Information

6.1.1 Under the Data Protection Act, individuals have the right to access information held about them and to correct any factual errors that may have been made. Where records are rectified, whether at the request of the individual or otherwise, any changes made must be recorded and communicated to all organisations with whom the information has previously been shared.

6.1.2 Individual members of the public on whom information is held, can request access to information of a personal nature (known as subject access requests). Generally individuals are given access to everything in their records but there may be some exceptions to this (e.g. where the record may also contain confidential information about other people).

6.1.3 Subject access requests should be sent to the relevant data controller and will be dealt with using the corporate guidelines which can be found on the Council's Data Protection pages.

6.2 Requests for Information

6.2.1 The Freedom of Information Act & the Environmental Information Regulations gives the public a right to request information. Any person who makes a request to a public authority for information must be supplied with that information, subject to certain exceptions. Most of the exemptions involve the application of a public interest test to determine whether the public interest is best served by withholding or releasing the information.

6.2.2 Any written request for information we receive should be processed in line with the legislation, even if it doesn't mention the Freedom of Information Act or Environmental Information Regulations. Requests may be received by individual services or may be sent to Legal Services who disseminates to the relevant service area/s.

6.2.3 All requests should be dealt with using the corporate guidelines which can be found on the Council's Freedom of Information pages.

7. GOVERNANCE

7.1 Notification

7.1.1 Under the Data Protection Act, organisations are required to provide the Information Commissioner's Office (ICO) with a description of whom they intend or may wish to disclose personal information to. The legal requirement is to provide a description of the types of organisation who will be in receipt of the information rather than individual cases or names.

7.1.2 When you intend to share personal information, you must check whether you need to update your notification to describe this. When any part of the notification entry becomes inaccurate or incomplete, for example because you are now disclosing information to a new type of organisation, you must inform the ICO as soon as practical and in any event within 28 days. It is a criminal offence not to do this.

7.1.3 Where several organisations are sharing personal information it is important that each organisation is clear about the personal information they are responsible for and include that information on their notification entry.

7.2 Privacy Impact Assessments

7.2.1 Before entering into any information sharing arrangement, a Privacy Impact Assessment (PIA) should be completed. This is to assess the benefits that the information sharing might bring & any risks or potential negative effects such as the likelihood of damage, distress or embarrassment being caused to individuals or the Council. Privacy Impact Assessments must be completed when introducing new processes involving personal information. Further information on how to complete a PIA is available from the ICO.

7.3 Information Sharing Agreements

7.3.1 An Information Sharing Agreement sets out a common set of rules to be adopted by the various organisations involved in an information sharing operation. An Information Sharing Agreement should be put in place when information is being shared between Data Controllers and could form part of a contract between organisations. It is good practice to regularly review an Information Sharing Agreement, particularly where information is to be shared on a large scale, or repeatedly.

7.3.2 An Information Sharing Agreement should, at least, document the following issues:

- the purpose, or purposes, of the sharing;
- the information to be shared;
- how the information will be shared;
- the potential recipients or types of recipient and the circumstances in which they will have access;
- information quality – accuracy, relevance, usability etc.;
- information security;
- retention of shared information;
- individuals' rights – procedures for dealing with access requests, queries and complaints;
- review of effectiveness/termination of the sharing agreement; and
- sanctions for failure to comply with the agreement or breaches by individual employees.

7.3.3 A template for an Information Sharing Agreement can be found here. This is to be used to support any exchange of information with another organisation/s. Guidance for creating an Information Sharing Agreement can be found as an appendix to the template.

7.4 Information Processing Agreements

7.4.1 Where information is to be shared with another organisation for them to process personal data on the Council's behalf, it must be supported with an Information Processing Agreement. When information is shared in this way, i.e. between a Data Controller and Data Processor, the Data Protection Act requires a written contract to be in place which states the specific instructions for which the information is to be processed and secured.

7.4.2 A processing agreement is designed to sit alongside or be integrated into a contract and details the specific requirements for handling information. It is essential to monitor an agreement to ensure that any external party with access to Council information is acting within the terms set out the agreement and the law. This is particularly important as the responsibility for the information remains with the Data Controller.

7.4.3 An Information Processing Agreement should, at least, document the following issues:

- the service to be provided;
- the information to be provided;
- the purposes for which the data will be used;
- exchange of information;
- information security;
- retention and destruction of processed information;
- dealing with subject access requests, queries and complaints;
- compliance and breaches of the agreement.

7.4.4 A template for an Information Processing Agreement can be found here. This is to be used when sharing information with another organisation in order for them to process it. Guidance for creating an Information Processing Agreement can be found as an appendix to the template.

7.5 Sharing Information between Departments

7.5.1 Sharing information within an organisation is different to sharing with another organisation. Under the Data Protection Act, the Council is a single entity which makes its own decisions on how personal information is used. However, the sharing of information must still adhere to the Data Protection principles. In particular, if one department holds information for one particular purpose and then passes it to another department so that it can be used for another purpose, this would be classed as a secondary use of that information (see data protection principle 2, Appendix 1).

7.5.2 Any secondary use of information must not be outside of what an individual would deem reasonable and individuals should be informed (if not asked for consent) of their information being processed in this way. This can be done at the point the information is collected by way of a privacy notice (see Fair Processing and Privacy Notices, section 5.2).

7.5.3 It is important to note that if the decision is made to share personal information with another department within the Council, all of the Data Protection principles will apply to the secondary set of information and any subsequent processing must remain fair and lawful.

7.6 Information Standards

7.6.1 It is important to have procedures in place to maintain the quality of the information you hold, especially when you intend to share information. When planning to share information with another organisation, you will need to consider all information quality implications.

7.6.2 When sharing information, you should check the following;

- The format of the information you share is compatible with the systems used by both organisations;
- The information you are sharing is accurate;
- Inaccurate information is corrected by all the organisations holding it;
- Common retention periods and deletion arrangements are set for the information you send and receive;
- Employees are trained so that they know who has the authority to share personal information and in what circumstance; and

- Both organisations are aware of how the information is to be transmitted and by whom

7.7 Information Sharing Review

7.7.1 Once information sharing arrangements are in place, they should be reviewed on a regular basis. This is because changes can occur and they need to be reflected in your arrangements to ensure that such sharing can still be justified. If it cannot be justified, it should stop.

7.7.2 The following questions should be looked at regularly;

- Is the information still needed?
- Does the privacy notice and Information Sharing Agreement (ISA) still explain the information sharing accurately?
- Are your information governance procedures still adequate and working in practice?
- Have you checked that you are still providing people with access to all the information they are entitled to?
- Have you checked that you are responding to people's queries and complaints to your sharing arrangements?
- Have any issues occurred?
- Are all the risks still evaluated correctly?

7.7.3 If changes need to be made to your information sharing arrangements, this needs to be publicised appropriately.

8. SECURITY

8.1 It is important that appropriate technical and organisational measures are in place when sharing information. Although the Council may be familiar with protecting its 'own' information, establishing appropriate security in respect of shared information may present new challenges.

8.2 It is good practice to take the following measures in respect of information that you share with other organisations, or that other organisations share with you:

- Assess whether you share any information that is particularly sensitive and ensure that this is subject to appropriate security measures and necessary protective marking; identify who has access to information that has been shared with you; 'need to know' principles should be adopted. Not all employees should be given access if only a few of them need it to carry out their job;
- Consider the effect a security breach could have on individuals and the Council; and
- Consider the physical and technical security measures and assess whether they are adequate for the information received.

8.3 Information Exchange

8.3.1 The method of exchanging information should always be the most secure available. The ways in which you may choose to exchange information are set out below:

Email

Email is only secure if the e-mail system itself is secure. Where available, users should use a secure email account (GCSx) but only if the recipient also has a secure account. Encryption and password protection also provide security when using standard email systems.

Note: The encryption software in use by the Council is 7-Zip. Guidance on encrypting files using 7-Zip is available here.

Fax
This is not a recommended method of exchanging information. This should be used as a last resort and only if the person receiving the information is waiting at the machine. Do not assume this will always be the case and ensure they are waiting for your fax before it is sent. A cover sheet must be used when transmitting protected information via fax and the recipient be notified that the information is about to be sent and must confirm that the information has been received.

Paper Exchange
Paper copies of information can be exchanged in person provided that both the information holder and the recipient take appropriate measures to ensure that the information cannot be read by any unauthorised persons. If information has to be sent via post, it is recommended that a method is used that ensures the delivery of the mail and allows it to be tracked (e.g. recorded delivery).

Verbal Exchange
This method is only secure if given to those who are authorised to hear it, or it is not overheard when exchanged or discussed (e.g. in a busy office). If information is exchanged verbally in a manner where it is not recorded at the time, the exchange should be validated and confirmed in writing as soon as possible.

Note: Verbal information should be subject to the same considerations as written, and should not be exchanged unless both parties are satisfied that the request is legitimate and there is a good reason for not exchanging the information in a written format.

8.4 Breach of Security

8.4.1 All agencies who are party to Information Sharing/Processing Agreements should have appropriate measures in place to investigate and deal with a potential or actual breach of security.

8.4.2 In the event that personal information shared under this protocol is or may have been compromised, the organisation making the discovery must:

- Inform the organisation who provided the information;
- Take steps to investigate the cause;
- Take disciplinary action against the person(s) responsible (if appropriate);
- Take appropriate steps to avoid a repetition;
- Take appropriate steps to mitigate any impacts.

8.4.3 In all instances, a breach of information security should be reported reported to your line manager and/or the Risk and Insurance Manager and/or Legal Services

8.4.4 Where a breach is identified as serious, it may have to be reported to the Information Commissioners Office (ICO). In this instance, both organisations (the original information provider along with the breaching organisation) will need to notify and may both be subject to enforcement action. Prior to any contact with the ICO, it must be discussed with the Risk and Insurance Manager and/or Legal Services

Appendix 1

The Data Protection Principles

The 8 Data Protection Principles are as follows;

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless;

    a) At least one of the conditions in Schedule 2 is met; and
    b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of the data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This is not a full explanation of the principles. For more information, refer to the ICO's website