APPENDIX 2

Tameside Metropolitan Borough

# Data Protection/Information Governance Conduct Policy

**Date: August 2021**

**Version: V2.0**

# Document Version Control

| Document Version Control | |
|---|---|
| Issue Number | Date |
| 1.0 | May 2018 |
| 2.0 | Approved by Information Governance Group - 7 September 2021 |
| 2.0 | Audit Panel Approval - 28 September 2021 |

# Contents

## 1. INTRODUCTION

1.1. Tameside Metropolitan Borough Council (the Council) has a responsibility under the Data Protection Act 2018 ("DPA 2018") and General Data Protection Regulations ("UK GDPR") to ensure that the information (including personal data) it holds and uses is properly protected. To this effect a Data Protection/Information Governance Framework, which is detailed in **Appendix 1**, has been created to support employees in complying with this responsibility.

1.2. This conduct policy forms part of the Framework and outlines what constitutes acceptable and unacceptable conduct by employees in respect of data protection/information governance.

### 1.3. Definitions

| Term | Definition |
|---|---|
| **Personal Data** | Is any personal data as defined by UK GDPR and the Data Protection Act 2018.<br>It is defined in the Data Protection Act 2018 at **s.3(2)** as "any information relating to an identified or identifiable living individual". Broadly this means any information (relating to a living individual who can be identified or identifiable, directly from the information in question, or indirectly identified from that information in combination with other information that is in the possession of the Council.<br>The UK GDPR provides a non-exhaustive list of identifiers, including:<br>• Name;<br>• Identification number;<br>• Location data; and<br>• Online identifier (e.g. IP addresses).<br>Personal data also applies to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living person.<br>The Council is legally responsible for the storage, protection and use of personal data/information held by it as governed by UK GDPR and the Data Protection Act 2018. |

| Term | Definition |
|---|---|
| **Special Category information** | This data is covered by Articles 6 and 9 of the General Data Protection Regulations (UK GDPR). As it is more sensitive it needs more protection and consists of:<br>• Racial or ethnic origin<br>• political opinions/beliefs<br>• religious or philosophical beliefs<br>• trade union membership<br>• genetic data<br>• biometric data (where used for ID purposes)<br>• health;<br>• sex life; or<br>• sexual orientation. |
| **Information** | Information can include all forms including, but not limited to:<br>• Hard copy or documents printed or written on paper;<br>• Information or data stored electronically, including scanned images;<br>• Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;<br>• Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;<br>• Information stored on portable computing devices issued by the council including mobile telephones, PDA's, tablets and laptops;<br>• Information stored in a cloud environment;<br>• Speech, voice recordings and verbal communications, including voicemail and any recordings from Online Virtual Meetings such as Skype, Teams and Zoom.<br>• Published web content, for example intranet and internet (Including Social Media Platforms).<br>• CCTV/Dashcam/Bodycam footage.<br>• Video and Photographs that allow an individual to be identified. |
| **Employee** | Includes all full and part-time employees, Members of the Council, temporary staff, volunteers, contractual third parties, partners or agents of the Council who have access to any information systems or information for Council purposes. |

1.4. This conduct policy also indicates the various supporting policies, protocols and procedures the Council has put in place to keep its information (including personal data) safe.

1.5. The policy applies to both work related and personal online activity and sits at the heart of the Data Protection/Information Governance Framework.

1.6. The DPA 2018 and UK GDPR are the key pieces of legislation covering personal information. The Information Commissioner's Office (ICO) is the UK regulator and has a range of enforcement actions including the power to fine organisations up to £17.5 million or 4% of annual turnover (depending on which is larger) for non-compliance.

1.7. The Local Public Services Data Handling Guidelines Sixth Edition (March 2021) outline best practice for protecting information together with resources provided by the Records Management Society, National Archives, Society for Innovation, Technology and Modernisation (SOCITM), National Local Authority Warning, Advice and Reporting Point (NLAWARP), NHS Data Protection and Security Toolkit, Local Authority Information Governance Groups and the Information Commissioners Office (ICO).

## 2. PROCEDURES

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

2.2. **Appendix 1** provides a list of each element of the Data Protection/Information Governance Framework with a brief explanation of the content of each of the supporting policies, protocols and procedures and an outline of acceptable and unacceptable conduct as set out in those documents. **Appendix 1** provides a summary only and all employees are required to familiarise themselves with the full text of those documents as appropriate for their job roles and duties.

2.3. These policies, protocols, procedures and guidance documents, which may be amended from time to time, are available on the Council's Intranet (Staff Portal) https://intranet2.tameside.gov.uk/infogov or on request from the Information Governance Team via email at Information.governance@tameside.gov.uk

2.4. The table shown in **Appendix 2** identifies the mandatory minimum documents for employees to read relevant to their role. It is the responsibility of Managers to ensure the appropriate documents have been communicated and read and to allow employees appropriate time to understand their responsibilities towards Data Protection/Information Governance and to provide clarification for employees of the relevant role if there is any doubt.

## 3. ROLES AND RESPONSIBILITIES

### 3.1. Manager Responsibilities

3.1.1. Managers are responsible for ensuring that new and existing employees have appropriate time and support to read the relevant documents and undertake any necessary and/or mandatory training on an annual basis. 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 Information Governance Team for advice and support at (information.governance@tameside.gov.uk).

3.1.2. It is the responsibility of Managers to exercise an appropriate supporting and enforcing role for the identified requirements of the Data Protection/Information Governance Framework to minimise the risk of data loss, destruction, inappropriate disclosure and breaches of legislation, especially in areas of high risk, where personal data is critical to service delivery.

### 3.2. Employee Responsibilities

3.2.1. 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 data/information (including personal data) they handle. It is the responsibility of all employees to ensure their use of the Council's data/information does not infringe any of the Council's policies and procedures, or, in turn breach the requirements of the DPA 2018, UK GDPR, the Freedom of Information Act 2000 ("FOIA 2000") and the Environmental Information Regulations 2004 ("EIR 2004") or any other applicable legislation.

3.2.2. Employees have a responsibility to comply with the Data Protection/Information Governance framework, when not only handling personal data but also when generally using the internet, any electronic communication or social media. The policies and procedures and guidance detailed in **Appendix 1** will assist with this compliance.

3.2.3. Employees have a responsibility to comply with mandatory Data protection/information governance training and to meet the deadline set as this is a council wide objective. Failure to complete the training in the set timescale could result in Disciplinary Action.

3.2.4. The public is entitled to expect the highest standards of conduct from Council employees, when handling personal data/information. The 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 Data Protection/Information Governance Framework and data protection legislation.

3.2.5. There is an expectation that all communication from staff, whether handwritten, electronic or verbal, is done so with a high level of professionalism. All communications should meet the 'Chief Executive Test' namely would the Chief Executive say or write this on behalf of the Council or more importantly would this communication give the Chief Executive cause for concern if he saw it? All communication, whether written or verbal should be courteous and in a style appropriate to business communication and not in a casual or flippant tone. Careless or casual use of humour/Emoji's 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. Any written information can be requested under Subject Access or Freedom of Information Request, so staff need to think what the impact would be on an individual if they read that information or it was disclosed to a third party. Any notes taken should be contemporaneous (written at the time the piece of work/meeting/call/discussion was carried out or as soon after as is reasonably practicable) and be factual rather than containing the author's personal opinion.

## 4. HOW WE MANAGE BREACHES OF THE POLICY

4.1. Employees need to be aware that this policy and the documents that make up the Data Protection/Information Governance Framework are in place to protect the information held by the Council and to provide assurance to partners, key stakeholders, service users, customers and the residents of Tameside. Failure to adhere to these framework policies, protocols, procedures and guidance documents may lead to disciplinary action being taken against any employee(s) involved and for more serious cases, where employees have not followed guidance and policies, legal action may be taken. For further information please read the "Disciplinary Procedure" on the Council's HR Policies and Procedures page here.

4.2. All employees **must** report any suspected or actual data breaches or any breaches of this conduct policy, or any of the other Data Protection/Information Governance Framework policies to their line manager **<u>and</u>** the Information Governance team as soon as they become aware, in line with the Personal Data Breach Reporting Procedure.

4.3. In addition it should be noted that the Information Commissioner's Office (ICO) may also take action in cases where these policies have been breached. The ICO may take action against the Council as an organisation, but can also take action against any individual employee(s) involved. This can include the imposition of a fine of up to £50,000 against any individual and the ICO may also seek to privately prosecute any individual in the event that they purposefully used data/information for their own financial or personal gain or acted in a highly negligent/reckless manner.

**APPENDIX 1**

## DATA PROTECTION/INFORMATION GOVERNANCE FRAMEWORK

### 1. Data Protection/Information Governance Policy and Conduct Policy

The Data Protection/Information Governance Policy and Conduct Policy are central to the Data Protection/Information Governance Framework and must be read by all employees.

The purpose of these policies are to protect the Council's information assets from all threats, whether internal or external, deliberate or accidental. Additionally, the conduct policy outlines what constitutes acceptable and unacceptable conduct by employees in respect of data protection/information governance

Further guidance on the information contained within these documents can be found in the supporting framework documents and a Data Protection/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.

All employees **must** report any suspected or actual data breaches or any breaches of any of the Data Protection/Information Governance Framework policies to their line manager **and** the Information Governance team as soon as they become aware, in line with the Personal Data Breach Reporting Procedure.

To view the Data Protection/Information Governance Policy, click here.

### 2. Appropriate Policy Processing Special Category Data

This document sets out how special category data and criminal offence data will be processed by the Council and how those categories of personal data will be protected in line with Schedule 1 of the Data Protection Act 2018.

Acceptable Conduct

All employees **must:**

- Follow this policy for all processing of personal data throughout the Council;
- Protect any personal data within their care;
- Seek additional advice and guidance from their manager, the Information Governance Team or the Data Protection Officer if unsure or in any doubt about how to handle personal information;
- Keep up to date with all Council Data Protection and Information Governance training that is appropriate to their role.

For further guidance click here

### 3. IT 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. This policy is to be read in conjunction with the Access and Security Protocol.

Acceptable Conduct

- Protect, at all times, passwords which enable access to data and the Council's network, business systems, email and internet, and regularly update your passwords, ensuring that you do not use the same password across multiple systems. For further guidance refer to the IT Service Desk;

- Keep equipment, particularly portable equipment such as laptops, mobile telephones, PDAs and tablets, safe and secure at all times
- 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;
- Ensure that equipment and installed software is kept up to date with relevant patches and security fixes by regularly rebooting the equipment and installing any updates pushed out by ICT Services; and
- Always save work related information on the Council's network drives and not on local hard drives/desktop. The secure network is backed up and remains available even if your device fails.

For further guidance click here.

## 4. 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 only the level needed by the employee to perform their 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 whether it be temporary or permanent and managers are referred to the Leavers and Movers Checklist. As information is held in both paper and electronic format this procedure relates to both physical and technological access.

Acceptable Conduct,

- Access will only be granted 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 access necessary for the required purpose.

For further guidance click here

## 5. 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.

Acceptable Conduct

- Never open an email (or any attachments or links) 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 only;

- Never send protected information by external email **unless** you are using secure means. Emails sent between two ".gov.uk" accounts is generally deemed to be safe and does not require additional encryption, though employees are directed to check the Council's Safe to Send List prior to sending any protected information. All emails containing protected information sent to non .gov.uk recipients must be sent using Egress secure Mail. Consideration should also be given to using password protection on attachments (even where sent through Egress) for particularly sensitive information, though use of encrypted email is the minimum standard to be used;
- The Safe to Send List can be found here;
- Use of the Council's email and internet systems are monitored and activity is logged.

Unacceptable Conduct

- Using systems for personal use during working hours and it interfering with your day to day role
- Store any personal records on Council systems
- Emailing of curt, rude, sexually explicit, racially biased or offensive emails/communications (or attachments) and other inappropriate content.
- Using Technology to harass and abuse others at any time whether using council or own devices.

**Please note that Unacceptable Conduct could lead to personal criminal action under the Computer Misuse Act 1990 and also referral to any professional body you belong to.**

For further guidance click here

## 6. 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. All removable media must be procured via ICT Services. 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 Data Protection Act 2018 and General Data Protection Regulations (UK GDPR) and subsequent disciplinary action for the employees involved.

Acceptable Conduct

- Only encrypted USB memory sticks purchased through ICT Services may be used with Council equipment and IT systems. 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

## 7. 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 (laptops, tablets or PDAs) and static IT equipment. This is more important now as many of us are working remotely. All employees are responsible for the safety and security of portable devices and the information on them, issued to or used by them at all times. Explanations of what physical security is required on the devices and how to use them in line with Council policies and procedures are provided.

Acceptable Conduct

- Always ask yourself 'do you really need to take that information out of the office' and only take the minimum information required to complete your task;
- Do not let unauthorised people, including family members, use or view Council resources and avoid 'shoulder surfers' in public places and at home viewing your devices;
- When you leave your screen, make sure you lock it as if you were in an office environment, by pressing 'Ctrl + Alt + Delete' and then confirm that you wish to lock your workstation, or by pressing 'Windows key (⊞) + L';
- Whilst all Council issued devices are suitably encrypted, care should be taken to conceal equipment overnight as well as physical files, ideally in lockable storage;
- If you have a portable device (mobile telephone, tablet, PDA etc.) this should be password/pin code protected and locked at all times when not in active use;
- If attending meetings away from your workspace, reduce the risk by ensuring that any devices, files or papers are suitably concealed and therefore out of sight when not in use;
- Do not leave any equipment/files unattended in any vehicle.
- Remember if your workspace is outside others can listen/view. So beware of the content of your discussions.

For further guidance click here

## 8. 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.

Unacceptable Conduct

- 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 conducting themselves in a way that is detrimental to the Council and acting 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;
- Using 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
- Posting information that could constitute a breach of copyright or data protection legislation.

For further guidance click here

## 9. Social Media Investigations/Internet Research Policy

This document sets out corporate standards and instructions which will ensure that all online research and investigations are conducted lawfully and correctly in accordance with an individual's human rights and with due consideration of relevant legislation, including the Human Rights Act 1998 ("HRA 1998"), European Convention on Human Rights ("ECHR"), Data Protection Legislation (DPA 2018, UK GDPR etc.) and Regulations of Investigatory Powers Act 2000 ("RIPA 2000").

This policy and procedure should be read in conjunction with the Council's RIPA policies and procedures, which can be found here.

Acceptable Conduct

- Information gathered from social media can be useful when conducting investigations, **but** any investigations must be necessary for a specific and legitimate objective, proportionate to the objective in question, and carried out in accordance with the law.
- Any social media or internet research enquiries carried out under this policy must be attributable, overt, initial non-repeated research. Any research which is covert, likely to reveal private information and is carried out or repeated with some regularity over a period of time will fall under the RIPA policies instead. Repeated viewing (2 or more times) of "open source" information requires RIPA authorisation.
- Written activity records (audit trails) must be recorded in all cases of internet research, detailing the processes applied when obtaining the information and evidence.

For further guidance click here

## 10. Secure Workspace 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 DPA 2018 and UK GDPR subsequent disciplinary action for the employee could arise.

Acceptable Conduct

- 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 (whether in a TMBC office, public meeting space or working from home) using 'Ctrl + Alt + Delete' and then confirming that you wish to lock your workstation, or by using 'Windows Key (⊞) + L';
- At the end of the day, laptops and other portable equipment (mobile phone, tablets, PDAs) should be switched off. All portable equipment and any paperwork/files and/or removable media should be concealed when not in use. However, it is preferred if you are able to, to use a locked cupboard/drawers or store within a locked room. This policy applies to staff working at TMBC office premises and staff working from home; and
- When in any council owned premises, remove documents from printers and copiers as they are produced to avoid them being picked up by mistake, or read by someone else. Printing at home is not allowed;

- All waste paper and removable media which contains protected information must be disposed of appropriately and securely via the Council's confidential waste arrangements. Disposal of any hard copy or documents containing protected information (personal data, special category data or confidential information) or removable media at home is not allowed and all such items **must** be returned to Council premises for secure disposal.

For further guidance click here

## 11. Data Protection Impact Assessment

UK GDPR and DPA 2018 make 'data protection by design and default' an express legal requirement. The legislation expects that each data controller must implement appropriate technical and organisation measures to put data protection safeguards into place and minimise risk. It also makes 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is a process to help you initially identify, analyse, minimise and mitigate the risks associated with the processing of personal data or special category data involved with the projects and plans that the Council intends to carry out.

It is best practice to start a DPIA at project inception rather than at project delivery as DPIAs can take considerable time to complete, especially if any risks are identified that need action to reduce or mitigate to an acceptable level.

A DPIA is mandatory under UK GDPR and s.64 Data Protection Act 2018, where processing of data is likely to result in a high risk to the rights and freedoms of individuals. It is good practice to carry out a DPIA where there is any processing of Personal Data (including special category data) including video or images where a person could be identified.

A DPIA must:

- Describe the nature, scope, context and purpose of the processing;
- Assess necessity;
- Identify and assess risks to individuals;
- Identify additional, measures to mitigate risks.

The Information Governance team will provide advice and support to services when conducting a DPIA and they be contacted at an early stage on Information.governance@tameside.gov.uk.

The Information Governance team will review in conjunction with the service area and work towards sign off by the Senior Information Risk Owner ("SIRO"), who is the Head of Risk Management and Audit. If a DPIA is deemed high risk and cannot be adequately mitigated, the SIRO will liaise with the Data Protection Officer ("DPO"), who is the Director of Governance and Pensions (Borough Solicitor)) to achieve final sign off.

Acceptable Conduct

- A DPIA should be considered in the **early stages** of a proposed project or plan, before you start your processing of data, and run alongside the planning and development process. A screening checklist must be completed for any proposed project or plan in order to adequately assess the risks and determine the need for a full DPIA;
- The lead officer for the project or plan is the most appropriate person to undertake the DPIA, but they should also consult the Information Governance Team at an early stage. The lead officer should also consult ICT services, Legal services, system

providers, any joint controllers and any processors, where relevant and document this on the DPIA.

Unacceptable Conduct

- Failure to complete the DPIA screening checklist for any project started/refreshed since 2018.
- Failure to complete a DPIA for any project started/refreshed since 2018 that is subsequently found to be a high risk.

For further guidance click here

## 12. Information Sharing Protocol

Information sharing is essential in order to deliver better, more efficient public services. 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 DPA 2018 and UK GDPR and could result in disciplinary action.

Acceptable Conduct

- 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 trail of all decisions/disclosures.

Unacceptable Conduct

- Sharing Information that should have had a sharing agreement in place

For further guidance click here

## 13. Subject Access Request (SAR) Guidance

This guidance has been drawn up to assist employees in understanding how to recognise and respond to a SAR in compliance with the Council's obligations under DPA 2018 and UK GDPR. It explains the right of access to personal data and the procedures that must be followed.

Key Points

- Individual's data rights are set out in the DPA 2018 and UK GDPR.
- The right of subject access allows a living individual ("the data subject") to find out what information ("personal data") is held by an organisation about them and how it is processed;
- A SAR can be made verbally, or in writing (by post, email or through social media) and does not need to refer to the correct legislation/any legislation at all, or mention the phrase "subject access".
- All SARs should be responded to promptly, and in most cases the maximum time limit for responding to a SAR is 1 calendar month once the complete request has been received by the Council;

- Most SAR requests are sent directly to the Information and Improvement team (Executive Support), but if a service area receives a SAR request directly, they must refer it to informationandimprovement@tameside.gov.uk within 24 hours of receipt.
- In some cases exemptions may be applied, which means that certain information may not need to be disclosed to the data subject in response to their SAR;
- Where a requester is not satisfied with the response to their SAR, the Council offers an internal review. In addition to the internal review process, a data subject may also refer their complaint to the ICO, or may take action through the courts to enforce their right of subject access.

Acceptable conduct

- All SAR requests are referred to the Information and Improvement Team (informationandimprovement@tameside.gov.uk) within 24 hours of receipt.
- Processing and responding to a SAR within the statutory timescales.
- For all SAR requests relating to Children's Services and Adult's Services data, there is a designated SAR co-ordinator. All employees in those service areas must refer the SAR to the co-ordinator in addition to the Information and Improvement Team and assist the SAR co-ordinator where required.

Unacceptable conduct

- Persistent failure to respond to SARs within the statutory timescales.
- Failure to adequately or appropriately redact, or incorrectly applying redaction.

For further guidance click here

## 14. Records Management Policy

This policy enables service areas to manage their own records in an acceptable and appropriate manner in line with statutory, regulatory and best practice guidelines.

For further guidance click here

## 15. 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.

Acceptable Conduct

- Laptops and other portable equipment (mobile phones, tablets and PDAs) which are no longer required must be returned to ICT enabling the hard drive/internal storage 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'. Clear retention dates must be put in place on all physical and electronic data in line with statutory, regulatory and best practice guidelines for each service area and data must be reviewed prior to disposal to ensure that it is no longer needed.
- Knowing where your records are as a lost document can be considered as a data breach.

- Paper files can deteriorate over time. Some of these files are expected to be kept for a significant number of years – please consider deterioration of these files. Keeping minimal paper records is preferred.

Unacceptable Conduct

- A failure to follow the retention and disposal guidelines resulting in insecure disposal of data and/or retaining data for longer than permitted.

For further guidance click here

## 16. Personal Data Breach Reporting Procedure

This procedure must be applied immediately 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 a Personal Data Breach. All incidents, irrespective of scale, **must** be reported to the Information Governance Team (information.governance@tameside.gov.uk) within the first 24 hours of knowledge to allow for mitigations to be put in place, lessons to be learned and to improve data handling procedures and the breach response process.

Where a data breach is established to have occurred and there is a high risk of adversely affecting individuals' rights and freedoms, we are required to report to the Information Commissioners Office within 72 hours of first knowledge of the breach, without exception. Failure to report an incident to the Information Governance Team may result in disciplinary action being taken.

Acceptable Conduct

- You must always report actual, potential or suspected data breaches to the Information Governance Team at information.governance@tameside.gov.uk via the paper or online reporting form. You should also report to the Information Security Officer/Cyber Security Technical Specialist (Assistant Director Digital Tameside) and/or Legal Services, where relevant;
- In light of the short reporting timescales imposed by the ICO, in order to sufficiently investigate a potential breach and determine whether it requires reporting to the ICO, all service areas must co-operate fully with the Information Governance Team and give sufficient priority to any investigations to enable timely reporting to the ICO.

Unacceptable Conduct

- Failure to report an actual or potential breach within 24 hours of knowledge, or at all;
- Where a breach is considered high risk in terms of harm or volume of data subjects and/or needs reporting to the ICO;
- High Frequency of Incidents;
- Inappropriate Access to Council Systems/Records;
- Deliberate and/or unauthorised alteration of data;

For further guidance click here

**APPENDIX 2**

## DATA PROTECTION/INFORMATION GOVERNANCE FRAMEWORK MANDATORY DOCUMENTS MATRIX

| Framework Document | Managers | Office/ Home based employees, Mobile working employees and | Care Workers/Social Workers | Manual/ Outdoor Workers |
|---|---|---|---|---|
| Information Governance Policy | ✓ | ✓ | ✓ | ✓ |
| Information Governance Conduct Policy | ✓ | ✓ | ✓ | ✓ |
| Appropriate Policy Processing Special Category Data | ✓ | ✓ | ✓ | If Applicable |
| ICT Security | ✓ | ✓ | ✓ | ✓ |
| Access and Security Protocol | ✓ | ✓ | ✓ | ✓ |
| Email, Communications /Internet Acceptable Use Policy | ✓ | ✓ | ✓ | ✓ |
| Removable Media | ✓ | ✓ | ✓ | - |
| Mobile and Remote Working Protocol | ✓ | ✓ | ✓ | - |
| Social Media Policy | ✓ | ✓ | ✓ | ✓ |
| Social Media Investigations/Internet Research Policy | ✓ | ✓ | ✓ | If Applicable |
| Secure Workspace Procedure | ✓ | ✓ | ✓ | - |
| (DPIA) Data Protection by Design and Default Guidance | ✓ | If Applicable | If Applicable | - |
| Information Sharing Protocol | ✓ | If Applicable | If Applicable | - |
| Subject Access Request Guidance | ✓ | ✓ | ✓ | If Applicable |

| Framework Document | Managers | Office/ Home based employees, Mobile working employees and | Care Workers/Social Workers | Manual/ Outdoor Workers |
|---|---|---|---|---|
| Records Management Policy | ✓ | ✓ | ✓ | **If Applicable** |
| Retention and Disposal Guidelines | ✓ | ✓ | ✓ | **If Applicable** |
| Personal Data Breach Reporting Procedure | ✓ | ✓ | ✓ | ✓ |