APPENDIX 2

Information Governance Conduct Policy

May 2018

1. Introduction

1.1 Tameside Metropolitan Borough Council (the Council) has a responsibility under the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) to ensure that the personal information it holds and uses is properly protected. To this effect an Information Governance Framework, which is detailed 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, protocols 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 2018 and EU General Data Protection Regulations (GDPR) are the key pieces 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 €20,000,000 or 4% of annual turnover (depending on which is larger) for non-compliance.

1.5 The Local Public Services Data Handling Guidelines outline best practice for protecting information together with resources provided by the Records Management Society, National Archives, Society of Information Technology Management (SOCITM), 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 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, protocols, procedures and guidance documents, which may be amended from time to time, are available on the Council's Intranet (Staff Portal) or on request from Risk Management and Audit Services (Insurance).

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 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 2018 and EU General Data Protection Regulations (GDPR), the Freedom of Information Act 2004 and the Environmental Information Regulations 2004 or any other applicable legislation.

3.2 Employees have a responsibility to comply 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 detailed 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 Management and Audit Services (Insurance) 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. 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 Information Governance Framework.

3.6 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 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 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, 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.

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 residents of Tameside. Failure to adhere to these framework policies, protocols, procedures and guidance documents 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 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 Freshdesk Service;
- 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/desktop. 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 using Egress Switch 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) ***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 Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) 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

e) ***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 take 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

f) ***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

g) ***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,

- 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 necessary for the required purpose.

For further guidance click here

h) ***Incident 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 an Information Security Incident (ISI). All incidents, irrespective of scale, must be reported immediately 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. Where a breach is established to have occurred we are required to report to the Information Commissioners Office within 72 hours. Failure to report an incident may result in **disciplinary action** being taken.

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

i) ***Secure/Clear 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 Bill 2018 and EU General Data Protection Regulations (GDPR) 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

j) ***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 the DPA. It explains the right of access to personal data and the procedures that must be followed.

Key Issues

- Individual's data rights are set out in the Data Protection Bill 2018 and EU General Data Protection Regulations (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;
- 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;
- 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.
- A failure to follow this guidance may result in **disciplinary action**.

For further guidance click here

k) ***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.

For further guidance Click here

l) ***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.

For further guidance Click here

m) ***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 Bill 2018 and EU General Data Protection Regulations (GDPR) 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 click here

n) ***Data Protection Impact Assessment***

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

For further guidance click here

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, Communications /Internet Acceptable Use	✓	✓	✓	✓	✓	✓
Social Media Policy	✓	✓	✓	✓	✓	✓
Data Privacy Impact Assessments	✓	**If Applicable**	**If Applicable**	**If Applicable**	**If Applicable**	-
Removable Media	✓	✓	✓	✓	✓	-
Mobile/Remote Working	✓	✓	✓	✓	✓	-
Retention and Disposal	✓	✓	✓	✓	✓	-
Information Access Procedure	✓	-	-	-	-	-
Information Reporting Procedure	✓	✓	✓	✓	✓	✓
Secure/Clear Desk	✓	✓	✓	✓	✓	-
Bring your own Device	✓	✓	✓	✓	-	-
Information Sharing Protocol	✓	**If Applicable**	**If Applicable**	**If Applicable**	**If Applicable**	-
Golden Rules	✓	✓	✓	✓	✓	-
Managers Checklist	✓	-	-	-	-	-