Data Protection/Information Governance Policy

Date: March 2024

Version: V2.1

Document Version Control

Document Version Control		
Version Number	**Date**	**Approved by**
1.0	May 2018	Audit Panel – 29 May 2018
1.1	August 2021	N/a – consultation draft to Information Governance Group
2.0	September 2021	Audit Panel – 28 September 2021
2.1	March 2024	N/a – minor update to post holders of roles at paragraph 6.3 and removal of outdated framework diagram at section 3.

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

Contents

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 2018 (DPA 2018) and General Data Protection Regulations (UK GDPR) 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 has powers to enable them to impose monetary penalty notices on organisations for up to £17.5 million or 4% of annual turnover (depending on which is larger) for breaches of the DPA 2018 and UK GDPR along with having the authority to carry out assessments of organisations to ensure their processes follow good practice.

1.3. The key guidance documents that the Council would be measured against are UK GDPR, and the Local Public Services Data Handling Guidelines Sixth Edition - March 2021. The latter being produced by the Public Services Network in partnership with the Local Chief Information Officer Council, Society for Innovation, Technology and Modernisation (SOCITM) (formerly the Society of Information Technology Management, the Cabinet Office and the National Local Authority Warning, Advice and Reporting Point (NLAWARP). The Council therefore has an obligation to comply with these guidelines, to ensure good practice is being followed.

1.4. The DPA 2018 and UK GDPR detail requirements that must be complied with to ensure that the rights and freedoms of living individuals are not compromised, and that all personal data is processed in a secure and appropriate manner. The legislation also stipulates that those who record and use personal information must be open about how the information is used and must follow good handling practices. This applies to the whole lifecycle of information, including the collection, use, disclosure, retention and destruction of data. The Council is committed to fulfilling its obligations under this data protection legislation and has produced this policy to both assist officers and provide assurance to its customers.

2. PURPOSE OF POLICY STATEMENT

2.1. The purpose and objective of this Data Protection/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 data/information through preserving;

Confidentiality:	Protecting information from unauthorised access, use and disclosure by 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 usable on demand by an authorised individual, entity or process.

3. DATA PROTECTION/INFORMATION GOVERNANCE FRAMEWORK

3.1. This Data Protection/Information Governance Policy is the over-arching document of the Council's Data Protection/Information Governance Framework.

3.2. The Data Protection/Information Governance Framework comprises of the Data Protection/Information Governance Policy and specific supporting procedures, standards and guidelines as follows:

- Data Protection/Information Governance Policy;
- Data Protection/Information Governance Conduct Policy;
- Appropriate Policy Processing Special Category Data;
- IT Security Policy;
- Acceptable Use Policy
- Social Media Responsible Conduct Policy;
- Social Media Investigations/Internet Research Policy;
- Data Protection Impact Assessment (DPIA) - Data Protection by Design and Default Guidance;
- Data Sharing Code of Practice;
- Subject Access Request (SAR) Guidance;
- Redaction Guidance;
- Records Management Policy;
- Personal Data Breach Reporting Procedure.

4. SCOPE

4.1. Definitions

Term	Definition
Personal Data	Is any personal data as defined by UK GDPR and the DPA 2018. It is defined in the DPA 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. The UK GDPR provides a non-exhaustive list of identifiers, including: • Name; • Identification number; • Location data; and • Online identifier (e.g. IP addresses). 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. 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 DPA 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: • Racial or ethnic origin • political opinions / beliefs • religious or philosophical beliefs • trade union membership • genetic data • biometric data (where used for ID purposes) • health; • sex life; or • sexual orientation.
Information	Information can include 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 issued by the council including mobile telephones, PDA's, tablets and laptops; • Information stored in a cloud environment; • Speech, voice recordings and verbal communications, including voicemail and any recordings from Online Virtual Meetings such as Skype, Teams and Zoom. • Published web content, for example intranet and internet (Including Social Media Platforms). • CCTV / Dashcam / Bodycam footage. • 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.

4.2. Data Protection Principles

4.2.1. There are 7 key principles set out in the UK GDPR. These principles do not provide hard and fast rules but embody the spirit of the general data protection regime. Compliance with these principles is fundamental to embedding good data protection and is key to the Council compliance with the provisions of UK GDPR.

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose.
Data minimisation	Personal Data shall be adequate, relevant, and limited only to what is necessary in relation to the purposes for which it the data is processed.
Accuracy	Personal Data shall be accurate and where necessary kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.
Storage limitation	Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary. Personal data may be stored for longer periods insofar as the said personal data will be processed only for: • archiving purposes in the public interest; • scientific or historical research purposes; or • statistical purposes The above are permitted subject to appropriate technical and organisational measures being put in place to safeguard the rights and freedoms of the data subject(s) involved.
Integrity and Confidentiality	Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Accountability Principle	The Controller (the Council) shall be responsible for and be able to demonstrate compliance with all the above principles.

4.3. Overseas Transfer of Personal Data

4.3.1. Data should not be transferred to other countries that do not have the same level of data protection. Although this is not considered one of the GDPR principles, UK GDPR does require that organisations must receive explicit consent from their Data Subjects for their personal information to be transferred outside of the European Economic Area (EEA).

4.3.2. Based upon the UK GDPR principles, the Council will:

- Observe fully, conditions regarding the fair collection and use of personal information;
- Meet its obligations to specify the purpose for which information is used;
- Collect and process appropriate information, to the extent for which it is needed, to fulfil operational needs, or to comply with any legal requirements;
- Apply checks to determine the length of time that information is held;
- Take all appropriate security measures to safeguard personal information;
- Ensure the rights of data subjects, about whom information is held, are fully exercised;

- Ensure that all staff managing and handling personal information understand their contractual responsibilities;
- Ensure that all staff managing and handling personal information are appropriately trained;
- Ensure that all staff managing and handling personal information are appropriately supervised;
- Ensure that methods of handling personal information are regularly reviewed and evaluated;
- Ensure that personal information is not transferred abroad without the appropriate safeguards.

4.4. Personal Information Sharing

4.4.1. Any regular sharing of personal information between the Council and other agencies will be subject to an information sharing protocol, and an agreed data transfer process that meets the requirements of the DPA 2018 and UK GDPR. Personal information sharing with the Council must comply with the Data protection principles of 'Purpose' stating that personal data shall be obtained only for one or more specified or lawful purposes and shall not be processed in a manner incompatible with that purpose. Where information sharing, or contracting out of data processing, is envisaged a DPIA should be undertaken to review the proposed project and ensure proper due diligence is carried out.

4.5. Data Protection Impact Assessment (DPIA)

4.5.1. DPIAs are now mandatory under UK GDPR. A DPIA must be carried out for processing that is likely to result in a high risk to individuals. It is also good practice to carry out a DPIA for any major project that requires the collection and processing of personal data. A DPIA must:

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

4.5.2. It is important that DPIAs are completed early in any project to ensure adequate time is allocated to review the proposals and the impact on individuals and the Information Governance Team are available to support, advise and review the document throughout its lifecycle. Completed DPIAs need to be signed off by the Data Protection Officer, or the Head of Assurance on behalf of the Data Protection Officer. Requests for assistance should be emailed to the Information Governance Team at information.governance@tameside.gov.uk.

4.5.3. For further guidance, refer to the Data Protection Impact Assessment (DPIA) - Data Protection by Design and Default Guidance.

4.6. Consent

4.6.1. UK GDPR sets a high standard for consent as a lawful basis for processing personal or special category data. Where processing is based on consent, the Council is required to demonstrate that the Data Subject has consented to the processing of their personal data.

4.6.2. Consent requires either a positive opt-in process or a clearly written declaration of consent. Pre-ticked boxes or any other method of default approval cannot be used. The Data Subject has the right to withdraw their consent at any time where consent is the basis for processing personal data.

4.7. Data Subject Rights and Subject Access Requests (SAR's)

4.7.1. Data Subjects whose data is held by the Council have the following rights over their personal data and can access that data and any supplementary information about how their data is being processed, by submitting a Subject Access Request:

- The right to be informed about how and why their personal data is processed;
- The right to access their data (Subject Access Request);
- The right to rectify their data;
- The right to be forgotten – erasure of their data;
- The right to restrict processing of their data;
- The right to data portability;
- The right to object to processing of their data;
- The right to object to profiling, or automated decision making.

4.7.2. These requests must be handled and responded to in a timely manner in line with the requirements of GDPR which determines that all SARs must be:

- Provided free of charge;
- Answered without delay and within one calendar month;
- Provided in a clear, easily accessible format.

4.7.3. All SARs will be managed and tracked by the Information and Improvement Team (Executive Support).

4.7.4. For further guidance, refer to the Subject Access Request Guidance.

4.8. Training

4.8.1. All staff must receive information governance training at induction and when receiving a new device. Further training may be provided to particular roles as appropriate.

4.8.2. Information Governance professionals, IAOs and SIAOs should receive specialist training relevant to their role. Additionally, leaders and board members including the SIRO and Caldicott Guardian should receive suitable training.

4.8.3. Refresher training will be provided, as described in the supporting policies.

4.8.4. Awareness sessions will be provided to teams on request and regular reminders on information governance topics made available through corporate communication channels

5. DATA PROTECTION/INFORMATION GOVERNANCE

5.1. Data Protection/Information Governance is the overall process of analysing, evaluating, assessing and mitigating the impact of risks to an organisation's information and information systems. It includes physical, personnel, information security and technological solutions and is an essential enabler towards making the Council work efficiently and maintaining public trust. Data/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. Data/Information risks 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 Data Protection/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 (Directors, Assistant Directors and Service Unit Managers) have 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 Council Governance initiatives. 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 Sixth Edition (March 2021) and UK GDPR specify roles organisations must appoint to in relation to Information Governance as follows:

- Data Protection Officer (DPO);
- Accounting Officer;
- Senior Information Risk Owner (SIRO);
- Information Asset Owners (IAO).

6.3. These specific roles together with the Information Governance Group and Information Champions will work together with senior management to ensure compliance with best practice whilst maintaining the over-riding objective to keep the Council's data/information safe.

6.4. The table below details the roles and responsibilities allocated to key staff.

Data Protection Officer	The **Data Protection Officer** has the formal responsibility for regulating and approving the application of information legislation for the organisation. The **Data Protection Officer** is the **Assistant Director – ICT & Digital**.
Monitoring Officer	The **Monitoring Officer** is responsible for ensuring the lawfulness and fairness of Council decision making and must report on matters they believe are, or are likely to be, illegal or amount to maladministration. The **Monitoring Officer** is the **Assistant Director Legal/Borough Solicitor**.
Accounting Officer	The **Accounting Officer** has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. The **Accounting Officer** is the **Assistant Director of Finance**.
SIRO	The **Senior Information Risk Owner** has overall responsibility and accountability in all aspects of Data Protection including the overall Data Protection/Information Governance Policy and strategy. They are

	required to provide assurance that all risks are effectively managed and mitigated. The **SIRO** is the **Director of Resources**.
Caldicott Guardian	The **Caldicott Guardian** has overall responsibility for protecting the confidentiality of people's health and care information and ensuring it is used properly. The **Caldicott Guardian** is the **Director of Adult Services**
IAO	**Information Assets Owners** are Directors/Assistant Directors involved in running the relevant Directorate. Their role is to understand in their business area, what information is held, what is added and removed, how information is moved, and who has access and why. The IAOs address risks to the information assets they 'own' and provide assurance to the SIRO on the security and use of those assets. The IAOs ensure that the Council's Information Governance Policies are communicated and implemented within their respective areas of responsibility, and ensure that any issues regarding resourcing, training, and compliance are escalated to the DPO, the Information Governance Team, their Information Champion or the Information Governance Group.
SIAO	**Supporting Information Assets 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 IAOs on what information their service area holds and how it is being managed. The SIAOs should equally ensure that the Council's Information Governance Policies are communicated and implemented within their respective areas of responsibility, and ensure that any issues regarding resourcing, training, and compliance are escalated to their IAO.
Information Security Officer / Cyber Security Technical Specialist	The **Information Security Officer** and **Cyber Security Technical Specialist** are responsible for developing and implementing the Councils' Cyber Strategy, Information Security policy and associated policies and procedures, to reflect local and national standards and guidance and legislative requirements. They also ensure compliance with information security requirements. The **Information Security Officer** is the **Assistant Director – ICT & Digital.**
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.
Information Governance Group	The IGG is chaired by the Data Protection Officer and meets once every two months. The role of the IGG is to: • Decide and/or recommend operational matters around all aspects of Information Governance; • Establish a Framework to embed best practice in all aspects of Information Governance; • Define the organisational policies in respect of data protection considering any legal and local authority requirements;

	• Provide regular reporting to the SLT which should include any key risks relating to the Council's ability to demonstrate compliance to regulation/policies; • Provide an update on reported incidents of Personal Data Breaches, SARs, IGG actions, audit points and any other key points as agreed by the IGG members.
Information Champions	Information Champions are senior managers representing services from across each directorate and act as the liaison between the Information Governance Group and staff to ensure the framework, communications and training are effective and reach all staff.
Records Manager	The **Records Manager** has day to day oversight of records management within the Council and is responsible for developing and reviewing policy and procedures that ensure service areas store, monitor, update, and where appropriate destroy their records in compliance with policy and legislation.