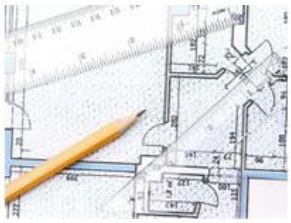
Tameside Metropolitan Borough

Data Protection Policy



May 2024

Version: 2.2

Document Control

Owner	Data Protection Officer
Author	Head of Assurance
Last Reviewer	Head of Assurance
Approver	Audit Panel
Date of Approval	25/06/2024
Date of Next Review	2025
Version	2.2
Classification	Public

Version Number	Date	Changes	Approved by
1.0	May 2018	Original Policy	Audit Panel
1.1	August 2021	Consultation with IGG	n/a
2.0	September 2021	Approval following consultation	Audit Panel
2.1	March 2024	Minor amendments for post holder changes	n/a
2.2	May 2024	Removal of IG Framework to separate document	Audit Panel

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 It supersedes any previous version of this document, which are now withdrawn.

Further information, advice or guidance about this document can be obtained from:
The Information Governance Team
information.governance@tameside.gov.uk

1. INTRODUCTION

1.1 Data 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 (ICO).

1.2 The ICO has powers to impose sanctions, including 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. 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 data must be open about how the data is used and must follow good handling practices. This applies to the whole lifecycle of data, including the collection, use, disclosure, retention, and destruction of data. The Council is committed to fulfilling its obligations under this legislation and has produced this Policy to both assist officers and provide assurance to its customers.

2. SCOPE

2.1 This Policy applies to all members, employees, apprentices, volunteers, contractors and third parties handling Council information. It is the responsibility of all to ensure compliance and adherence to this Policy, procedures, and guidance.

2.2 This Policy should be read in conjunction with the Information Governance Framework.

3. PERSONAL DATA

3.1 The DPA 2018 and UK GDPR relates to personal data.

3.2 **Personal data** is defined in the DPA 2018 at s.3(2) as:
"any information relating to an identified or identifiable living individual"

3.3 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.

3.4 The UK GDPR provides a non-exhaustive list of identifiers, including:

- Name;
- Identification number;
- Location data; and
- Online identifier (e.g. IP addresses).

3.5 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.

3.6 UK GDPR also defines personal data that is classified as **special category data**. This data is more sensitive data, 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.

3.7 The identified or identifiable living individual to whom personal data relates are **data subjects**.

4. DATA PROTECTION PRINCIPLES

4.1 There are seven key principles set out in the UK GDPR.

4.2 These principles do not provide hard and fast rules but embody the spirit of the general data protection regime.

4.3 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	The Controller (the Council) shall be responsible for and be able to demonstrate compliance with all the above principles.

5. COMPLIANCE WITH THE PRINCIPLES

5.1 Based upon the UK GDPR Principles, the Council will:

- Observe fully, conditions regarding the fair collection and use of personal data.
- Meet its obligations to specify the purpose for which data is used.
- Collect and process appropriate data, 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 data is held.
- Take all appropriate security measures to safeguard personal data.
- Ensure the rights of data subjects, about whom data is held, are fully exercised.
- Ensure that all staff managing and handling personal data understand their contractual responsibilities.
- Ensure that all staff managing and handling personal data are appropriately trained.
- Ensure that all staff managing and handling personal data are appropriately supervised.
- Ensure that methods of handling personal data are regularly reviewed and evaluated.
- Ensure that personal data is not transferred abroad without the appropriate safeguards.

5.2 Overseas Transfer of Personal Data

5.2.1 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 data to be transferred outside of the European Economic Area (EEA).

Personal Data Sharing

5.3 Any regular sharing of personal data between the Council and other agencies will be subject to a data sharing protocol, and an agreed data transfer process that meets the requirements of the DPA 2018 and UK GDPR.

5.4 Personal data sharing with the Council must comply with the Data Protection Principle 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.

5.5 Where data sharing, or contracting out of data processing, is envisaged a Data Protection Impact Assessment should be undertaken to review the proposed project and ensure proper due diligence is carried out.

Data Protection Impact Assessments (DPIAs)

5.6 DPIAs are 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.

5.7 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.
- Identify additional, measures to mitigate risks.

5.8 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.

5.9 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:

5.10 information.governance@tameside.gov.uk.

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

Consent

5.12 UK GDPR sets a high standard for consent as a lawful basis for processing personal data 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.

5.13 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.

5.14 The data subject has the right to withdraw their consent at any time where consent is the basis for processing personal data.

Data Subject Rights

5.15 Data Subjects whose data is held by the Council have the following rights over their personal data:

- The right to be informed about how and why their personal data is processed (transparency);
- The right to access their data and receive supplementary information about how their data is being used (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.

5.16 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.

5.17 All SARs will be managed and tracked by the Information and Improvement Team (Executive Support):
informationanddata@tameside.gov.uk

5.18 For further guidance, refer to the Subject Access Request Policy.

Training

5.19 All staff must receive data protection training at induction and when receiving a new device. Further training may be provided to particular roles as appropriate.

5.20 Information Governance professionals, Information Asset Owners and Supporting Information Asset Owners should receive specialist training relevant to their role. Additionally, leaders and board members including the Senior Information Risk Owner and Caldicott Guardian should receive suitable training.

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

5.22 Awareness sessions will be provided to teams on request and regular reminders on data protection made available through corporate communication channels.