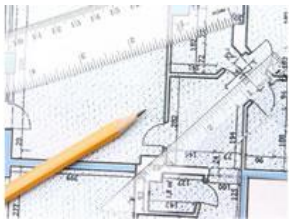
Tameside Metropolitan Borough

Information Governance Framework



June 2025

Version: 1.2

Document Control

Owner	Data Protection Officer
Author	Head of Assurance
Last Reviewer	Data Protection and Information Governance Compliance Manager
Approver	Audit Committee
Date of Approval	24 June 2025
Date of Next Review	30 June 2026
Version	1.2
Classification	Public

Version Number	Date	Changes	Approved by
1.0	April 2024	Original document	Audit Panel
1.1	11 March 2025	Updated to reflect change in governance structure and amendments to roles and responsibilities following IG service review	Audit Committee
1.2	24 June 2025	Amended wording at section 8.2 (roles and responsibilities) in relation to the DPO role to document why TMBC has appointed a DPO	Audit Committee

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 It supersedes any previous version of this document, which are now withdrawn.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. PURPOSE

1.1 To enable Tameside Metropolitan Borough Council (the Council) to meet its Information Governance obligations.

2. INTRODUCTION

2.1 Information is a core asset of the Council and is vital to ensure delivery of services and management of resources. It plays a key part in governance, service planning and delivery, and performance management.

2.2 Information Governance can mean different things to different people. It can be defined as the set of multi-disciplinary structures, policies, procedures, processes, and controls implemented to manage information, supporting the Council's immediate and future regulatory, legal, risk, environmental and operational requirements.

2.3 Information Governance can also describe the way we manage our obligations for accessing information, reuse of information, records management, surveillance, data protection, information security, Information Technology (IT) security, etc.

2.4 The Information Governance Framework comprises the policies and procedures of the Council which relate to Information Governance, roles and responsibilities, and sets out the governance and reporting arrangements.

3. SCOPE

3.1 This framework applies to all members, employees, apprentices, volunteers, contractors and third parties handling Council information.

3.2 It is the responsibility of all to ensure compliance and adherence to this framework and the supporting policies, procedures, and guidance.

4. LEGISLATION

4.1 The following legislation is relevant to the Information Governance Framework:

- Data Protection Act 2018 (DPA) – enables an applicant to access information of which they are the subject, e.g., someone's own education/social care records, employee files etc.

- UK General Data Protection Regulations (UK GDPR) – like the EU GDPR, provides safeguards to individuals over the processing of their personal information and setting requirements for organisations to ensure appropriate technical and organisational measures are in place to comply with the principles of data protection.

- Freedom of Information Act 2000 (FOIA) – enables an applicant access to information which is held by/on behalf of public authorities and those bodies carrying out a public function, and which does not fall under either of the access regimes i.e., personal information or environmental information.

- Environmental Information Regulations 2004 (EIR) – enables an applicant to access environmental information.

- Privacy and Electronic Communications Regulations 2003 (PECR) – sets out privacy rights relating to electronic communications, and covers electronic marketing, the use of website cookies, the security of public electronic communications services and privacy of users of electronic communications services.

- Re-use of Public Sector Information Regulations 2015 – establishes the UK framework for the re-use of public sector information. Accessible information which is produced, held, or disseminated by the public sector body must be made available for re-use (unless it is otherwise restricted or excluded).

- Regulation of Investigatory Powers Act 2000 - to make provision for the interception of communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; and for connected purposes.

- Computer Misuse Act 1990 - to make provision for securing computer material against unauthorised access or modification; and for connected purposes.

- Copyright, Designs and Patents Act 1998 - states the law of copyright; and for connected purposes.

- Human Rights Act 1998 - sets out the fundamental rights and freedoms that everyone in the UK is entitled to. It incorporates the rights set out in the European Convention on Human Rights (ECHR) into domestic British law.

- Equality Act 2010 – legally protects people from discrimination in the workplace and in wider society.

5. FRAMEWORK

5.1 The following key areas form part of the Information Governance Framework:

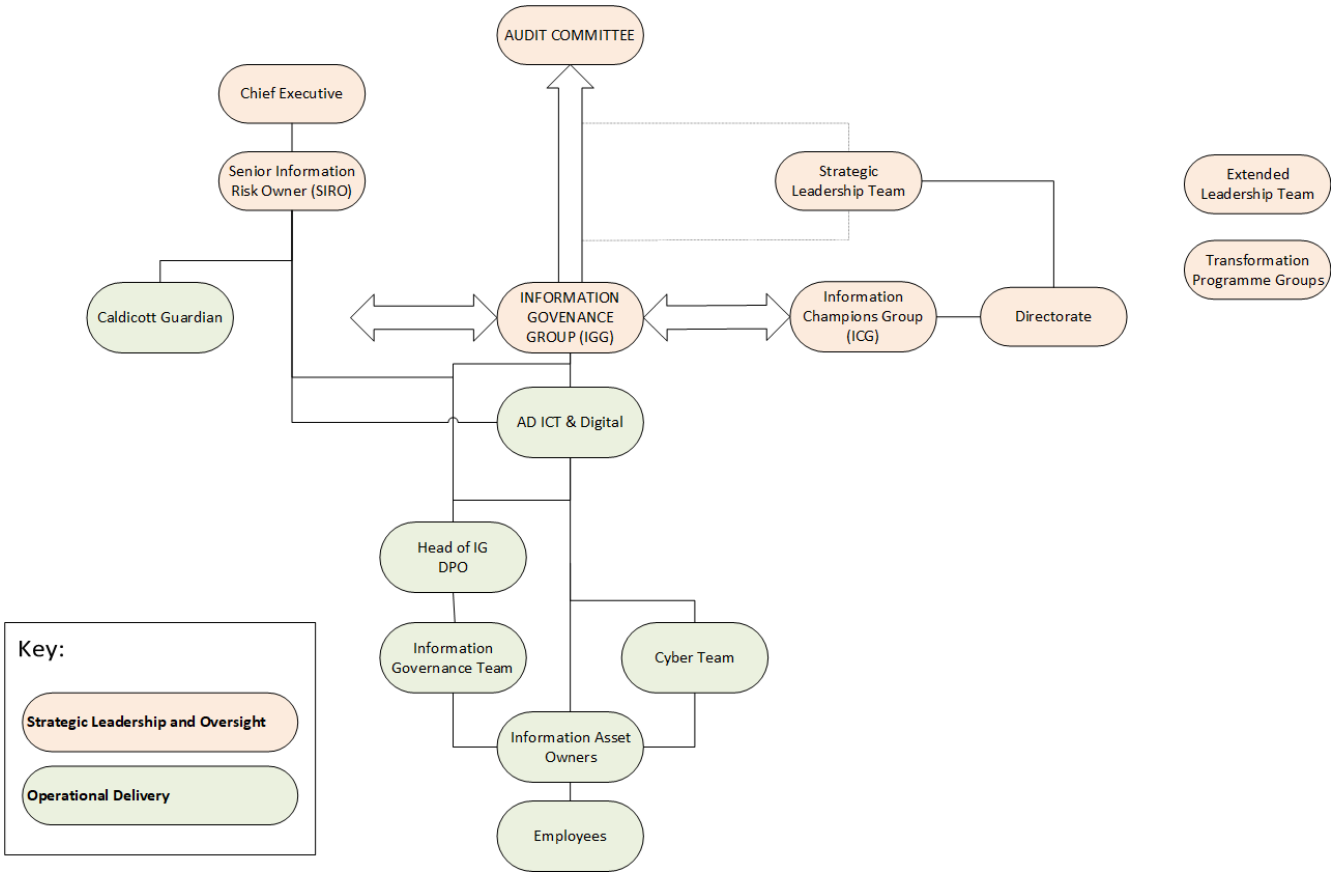
- Access to Information
- Data Protection
- Records Management
- Cyber

5.2 The Information Governance Framework diagram is located at **Appendix A**, which includes the list of policies, procedures, and guidance.

5.3 Further guidance on the information contained within these documents can be found in the Information Governance Framework Documents Matrix located in **Appendix B**, to assist managers and employees in assessing what documents are relevant to their role.

6. GOVERNANCE AND REPORTING

6.1 The following diagram illustrates the governance arrangements for the IG Framework:



Reporting

6.2 The Information Governance Team report to:

- Director of Resources/Assistant Director ICT & Digital on a weekly basis;
- All Directorates on a weekly basis regarding open FOI, EIR and SAR cases;
- Resources Directorate Leadership Team on a monthly basis;
- Strategic Leadership Team on a quarterly basis;
- The Information Governance Group in line with the Terms of Reference;
- The Head of Information Governance (Data Protection Officer) when required and as part of managing the service.

6.3 The Information Champions Group reports into the Information Governance Group.

6.4 The Information Governance Group reports into the Data Protection Officer via IGG meetings in line with the Terms of Reference and issues an annual report to the Audit Panel on IG activity.

7. TRAINING

7.1 All new starters must complete relevant mandatory training in respect of Information Governance, in line with the corporate Induction programme.

7.2 In addition, where required all officers must complete mandatory refresher training / new training as and when issued.

7.3 Where required, awareness sessions will be provided to relevant teams.

8. ROLES AND RESPONSIBILITIES

8.1 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:

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

8.2 The following table details Information Governance roles and responsibilities:

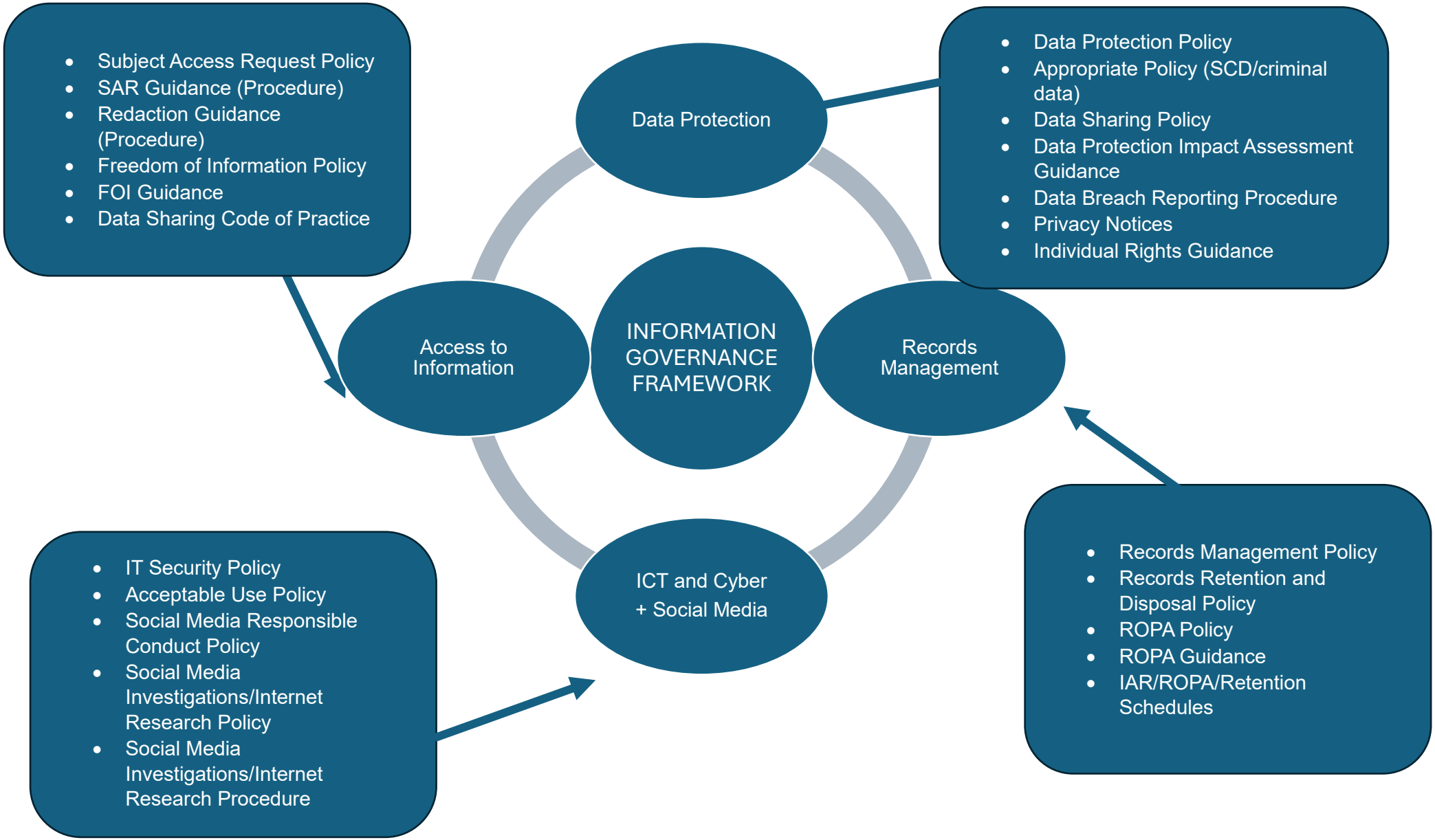
ROLE	RESPONSIBILITY
Elected Members of the Council	Complying with this Framework and associated policies, procedures and guidance, and the Member's Code of Conduct.
Audit Panel	To provide an independent and high-level focus on the adequacy of information governance arrangements.
Chief Executive	The Chief Executive has overall accountability for Information Governance.
Senior Information Risk Owner (SIRO)	The Senior Information Risk Owner has overall responsibility and accountability in all aspects of Information Governance. They are required to provide assurance that all risks are effectively managed and mitigated. The SIRO is the Assistant Director – ICT, Digital and IG.
Data Protection Officer (DPO)	In accordance with Article 37 UK GDPR, the Council as the Data Controller is a public authority and therefore required to have a Data Protection Officer (DPO). The Data Protection Officer has the formal responsibility for regulating and approving the application of information legislation for the organisation. The Council has assigned the role of the DPO to the Head of Information Governance.
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.

ROLE	RESPONSIBILITY
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.
Information Asset Owner (IAO)	The responsibility of Information Assets Owners is held by each of the Directors who are responsible for their respective Directorates. 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.
Supporting Information Asset Owner (SIAO)	Supporting Information Assets Owners are at Assistant Director and 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 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 Governance Group (IGG)	The IGG is chaired by the Data Protection Officer and meets every month. 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 Senior Leadership Team (SLT) which should include any key risks relating to the Council's ability to demonstrate compliance to regulation/policies • Provide an update an annual Information Governance report to the Audit Panel

ROLE	RESPONSIBILITY
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.
Information Security Officer and Cyber 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.
Head of Information Governance	The Head of IG has overall responsibility to lead and support the Information Governance function of the Council, overseeing the development and implementation of Information Governance and regulatory compliance strategies and ensuring that information risks are assessed and mitigated to an acceptable level. They also have management oversight for the operational team receiving and processing of requests for information in line with statutory and legal requirements. The Head of IG will also undertake the responsibilities of the Data Protection Officer (see above).
Data Protection and Information Governance Compliance Manager	The DP and IG Compliance Manager supports the Head of IG in managing the Data Protection area of the Information Governance Framework, supporting the delivery of the Information Governance Framework throughout the Council and ensuring there is robust information governance compliance in place in the Council. To deputise as required for the Head of Information Governance and ensure key tasks of the DPO are fulfilled.
Information and Records Manager	The Information and Records Manager has operational responsibility for ensuring that all requests for information received are handled in accordance with the relevant

ROLE	RESPONSIBILITY
	legislation, with the appropriate consideration of business risk to the organisation and ensure that Services are aware of the legal requirements placed upon them in respect of Information requests and complaints, police disclosure requests. 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.
Information Governance Officers	To deliver, under the direction of the DP and IG Compliance Manager and Information and Records Manager an Information Governance service for the Council. The IG Officers will ensure robust Information Governance compliance across the Council, ensure that the Information Governance framework is kept under review and remains fit for purpose and co-ordinate requests for information, working with services to provide sufficient response within statutory and legal requirements.
All Employees	Understanding and complying with this Framework, and the associated policies, procedures, and guidance, and the Employees Code of Conduct.

APPENDIX A – INFORMATION GOVERNANCE FRAMEWORK DIAGRAM



APPENDIX B - DOCUMENTS MATRIX

Framework Document	Managers	Hybrid / Home Working	Care Workers/ Foster carers	Manual / Outdoor Workers
Data Protection Policy	✓	✓	✓	✓
Appropriate Policy	✓	✓	✓	If Applicable
Data Sharing Policy	✓	If Applicable	If Applicable	If Applicable
IT Security Policy	✓	✓	✓	✓
Acceptable Use Policy	✓	✓	✓	If Applicable
Social Media Responsible Conduct Policy	✓	✓	✓	✓
Social Media Investigations / Internet Research Policy	✓	✓	✓	If Applicable
Social Media Investigations / Internet Research Procedure	✓	✓	✓	If Applicable
Data Protection by Design and Default Guidance	✓	If Applicable	If Applicable	If Applicable
ICO's Data Sharing code of practice	✓	If Applicable	If Applicable	If Applicable
Subject Access Request Policy	✓	✓	✓	If Applicable
Subject Access Request Guidance	✓	✓	✓	If Applicable
Redaction Guidance	✓	✓	✓	If Applicable
Freedom of Information Request Policy	✓	✓	✓	If Applicable
Records Management Policy	✓	✓	✓	If Applicable

Framework Document	Managers	Hybrid / Home Working	Care Workers/ Foster carers	Manual / Outdoor Workers
Retention and Disposal Policy	✓	✓	✓	If Applicable
Records of Processing Activity (ROPA) Policy	✓	If Applicable	If Applicable	If Applicable
Records of Processing Activity (ROPA) Guidance	✓	If Applicable	If Applicable	If Applicable
Records of Processing Activity (ROPA) (incorporates Retention Schedule)	✓	✓	✓	If Applicable
Personal Data Breach Reporting Procedure	✓	✓	✓	✓