TORBAY COUNCIL

Information Governance Framework

2020

Contents

This document can be made available in other languages and formats.

For more information please contact infocompliance@torbay.gov.uk

Document Control:

Organisation	Torbay Council
Creator	Head of Information Governance
Approvals	Information Governance Steering Group
Distribution	Corporate
Owner	Information Governance Steering Group
Protective Marking	Unclassified
Review due date	Sep 2022

Document Amendment History

Version No	Originator	Date of Change	Change description
1.1	Jo Beer	Feb 2017	Review
1.1	Information Governance Steering Group	March 2017	Framework approved.
2	Jo Beer	April 2018	GDPR Review and update
2.1	Jo Beer	Sep 2020	Review and update

1. Introduction

Information is a vital asset for the provision of all of Torbay Council's services to the public, it is vital in managing the Council's resources efficiently and effectively. Information has a key role in service planning, performance management and the Council's governance arrangements.

Information governance is concerned with how information is obtained, held, used and shared by the Council. This information can be held in both electronic and hard copy format.

Having a robust information governance framework in place helps ensure that information is effectively managed, appropriately shared, and that there are clear accountability structures in place, clear processes and documented policies and procedures.

The purpose of this document is to set out the Council's Information Governance Framework, to promote a culture of good practice in relation to information management and to help ensure that all staff are aware of their roles and responsibilities.

This framework is underpinned by the following legislation:

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- The Re-use of Public Sector Information Regulations 2005

2. Roles and Responsibilities

Chief Executive and Senior Leadership Team

The Chief Executive and the Senior Leadership Team (SLT) have ultimate responsibility for ensuring the delivery of an effective council-wide information management approach. They must ensure that the Council meets its responsibilities under the legislation outlined above.

Caldicott Guardian

The Caldicott Guardian is a senior officer responsible for protecting the confidentiality of information about service users as well as enabling appropriate information sharing, specifically in relation to information processed by social care services. They should act as the conscience of an organisation, considering whether processing activity and information sharing is the right thing to do.

Senior Information Risk Owner (SIRO)

The SIRO should be a senior manager who is familiar with information risks and the organisation's response to risk. The role of the SIRO is to take ownership of the organisation's information risk policy and act as an advocate for information risk.

The SIRO's responsibilities are:

- Leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers
- Owning the organisation's overall information risk policy and risk assessment processes and ensuring they are implemented consistently
- Owning the organisation's information incident management framework.

Data Protection Officer

The Data Protection Officer is an independent officer responsible for informing and advising the organisation and its employees of their obligations under data protection legislation.

They are responsible for:

- Monitoring compliance with current legislation and regulation and the Council's own policies in relation to the protection of personal data
- Awareness-raising and training of staff
- Investigating breaches of personal data
- Carrying out audits
- Providing advice on data protection matters including the completion of Data Protection Impact Assessments.
- Making recommendations to SLT about improvements to process
- Acting as the contact point for the Information Commissioner's Office
- Ensuring the Information Commissioner's Office is notified of any data breaches within 72 hours of them being reported.

Information Governance Team

The Information Governance Team supports the organisation to ensure compliance to Access to Information legislation including the Freedom of Information Act and Environmental Information Regulations. They also support the Data Protection Officer in delivering the required duties under data protection law. The team offer advice and guidance across the whole Council and support officers with information governance matters.

IT

The Council's IT department are responsible for ensuring that there are adequate security systems in place to keep our systems and the information we hold safe, this includes back-up and recovery procedures, access control policy, web and email policy among the other Information Security Policies. The Network Support Manager is the lead officer responsible for IT Information Security.

Information Asset Owners

Information Asset Owners are managers / heads of service involved in the running of the service. Their role is to determine how information is processed in their services and to understand what information is held, why it is held, what is added and what is removed, how information is moved, and who has access and why. They are also responsible for their entries on the Council's Information Asset Register.

All Managers

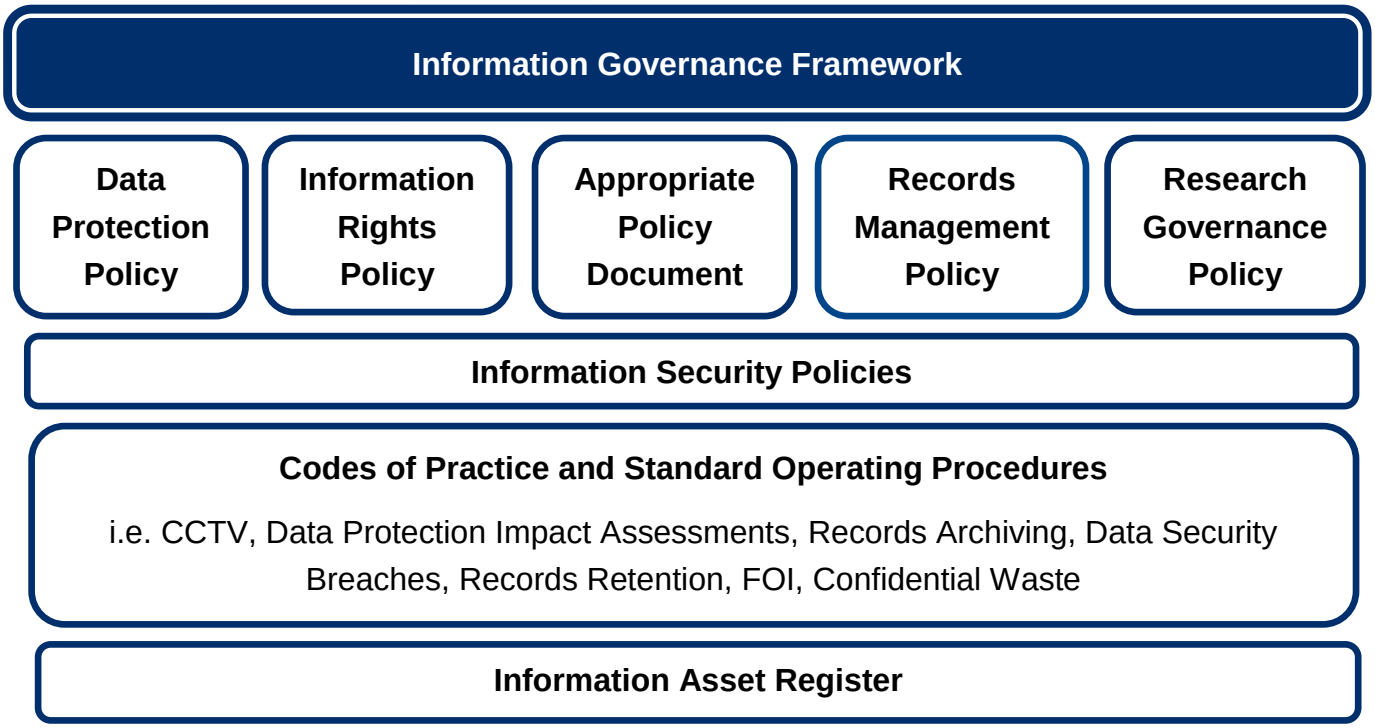
All managers must ensure their staff are provided with the relevant tools, guidance and training to process personal information in accordance with current data protection legislation and the Council's policies. Managers must ensure compliance in the day to day operation of service delivery and raise any issues or concerns with the Data Protection Officer. They must also take overall responsibility for the completion of Data Protection Impact Assessments. Managers must ensure that any recommendations made by the Data Protection Officer are actioned within the set timescales. In handling requests to share information, managers must consult with Information Governance to ensure disclosure is appropriate and lawful.

All Staff

All staff must ensure they comply with the Council's policies relating to Information Governance and Data Protection. Staff should raise any concerns they have with their manager, Information Governance or the Data Protection Officer, including the identification of any training needs. In handling requests to share information, staff must consult with Information Governance to ensure disclosure is appropriate and lawful. Staff must advise their manager and the Data Protection Officer immediately if they become aware that there may have been a personal data breach.

3. Key Policies

This framework acts an umbrella to a wider range of operational policies, codes of practices and operating procedures that all departments across the Council must be familiar with and comply with. The Council's framework of policies is shown below:



4. Structure

Information Governance Steering Group

The Information Governance Steering Group (IGSG) is made up of the Caldicott Guardian, the SIRO, the Data Protection Officer and other key officers representing departments across the Council. They meet on a six weekly basis and the purpose of the group is to take a strategic overview of information governance matters across the Council. They are responsible for:

- Ensuring that there are appropriate information governance policies and procedures in place
- Reviewing and approving data protection impact assessments where appropriate and monitoring risks and mitigations associated with ongoing and future high risk data processing
- Monitoring information handling, data sharing and breaches
- Reviewing recommendations from audits and breaches and ensure they are implemented
- Identifying emerging risks associated with systems and information assets and escalating any concerns to the Senior Leadership Team
- Monitoring and reviewing the Council's suite of policies relating to information governance, data protection and information security
- Championing information governance and data protection best practice across the Council.

It may be appropriate at times for smaller sub-groups to be formed outside of the main IGSG to look at specific matters such as information security policies, large projects, records management, and information risk. These sub-groups would be created as task and finish groups and will report to the IGSG.

5. Information Assets and Impact Assessments

In order to understand and monitor the risks associated with the information the Council holds an Information Asset Register. This register sets out information assets held across all services. This information asset register also acts as the Council's Records of Processing Activities which is required under Article 30 of the GDPR. The register sets out who holds what information, our lawful basis for processing that data, what the asset contains, who has access to the information and how the information is stored.

Information assets will inform the Council's information risk register and issues of concern will be reported to the Information Governance Steering Group and SIRO.

The Council is also committed to ensuring that Data Protection Impact Assessments (DPIAs) are undertaken when new systems are being procured, when a service is changing its processes which may change what information is being collected and when new information about our customers is being collected. These impact assessments allow officers to consider a project and identify any risks in relation to data protection and information governance associated with that project. The Data Protection Officer must be consulted on these impact assessments and approve them alongside the SIRO. The Council's policy regarding DPIAs is set out within the Data Protection Policy.

6. Training and Awareness

Information Governance training is provided to all staff through mandatory online i-learn modules which must be taken every year. It is expected that this training is undertaken by all staff, this includes secondees, agency and voluntary staff.

All new staff, as part of their induction, are provided with data protection training and all new social workers receive training on data protection as part of their Children's Services induction. Service specific training is also provided to staff / teams if necessary and where the findings from breach investigations identify training is required.

Through staff news, communicated by email, staff are regularly kept up to date with information governance and information security topics. Information about information governance, data protection and related policies can all be found on the council's intranet pages.

Torbay Council is committed to ensuring that staff are appropriately trained in the systems that they are using.

7. Information Sharing

Torbay Council is committed to sharing information where is appropriate and right to do so.

Information sharing is vitally important in protecting and safeguarding vulnerable children and adults and for the prevention and detection of crime. In this respect the Council will ensure that in accordance with the Caldicott 2 principles, information sharing is not a barrier and enables us to protect our vulnerable customers as well as making sure we are able to provide the services our customers need.

Where information is shared on a regular and consistent basis then the Council will ensure that appropriate information sharing agreements are in place, which set out clearly what information is to be shared, the legal basis under which information can be shared, the purpose for the agreement and the procedure for information sharing.

In cases where the Council receives requests for information about specific individuals from another organisation, the Council will consider the request and whether it is appropriate to share the information in accordance with data protection legislation.

Similarly, the Council may request information from other organisations and will ensure that any requests are appropriate and for a specific purpose which has been clearly outlined.

8. Monitoring and review

This policy and those policies which sit underneath this framework will be reviewed every two years and updated accordingly.

For further information please contact Infocompliance@torbay.gov.uk