TORBAY COUNCIL

U01 Corporate Information Security Policy

2020

Target Audience: Corporate

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

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

Contents

Document Control 1

1. Statement of Purpose 3

2. Scope of the Policy 3

3. Roles and Responsibilities 3

4. Security Management 4

5. Compliance 5

6. Dissemination of policy 6

7. Review of the Organisational Policy 6

Document Control

Organisation	Torbay Council
Title	Corporate Information Security Policy
Creator	Information Security Group
Approvals	Information Governance Steering Group
Distribution	Corporate
Owner	Information Governance Steering Group
Protective Marking	Unclassified
Review due date	16/10/2022

Document Amendment History

Revision No.	Originator of change	Date of Change	Change Description
1	Info Security Group	17/10/2011	Review
1.1	Kelly Prince	14/05/2013	Change of terms
2.1	Joanne Beer	16/10/2020	Full review, merged Information Security policy and organisational policy

1. Statement of Purpose

1.1 Information is a vital asset that Torbay Council has a duty and responsibility to protect.

1.2 The purpose and objective of this Organisational Policy is to set out the strategic responsibility for Information Security across Torbay Council.

2. Scope of the Policy

2.1 This policy applies to all Council staff and Members; to partner agencies and third parties and agents of Torbay Council, where specified by agreement, who have access to information systems, and/or, hold and process information for Torbay Council purposes. It applies to all information assets of the Council, where the council is the data controller.

2.2 Contravention of this policy may lead to disciplinary action, up to and including dismissal in very serious cases.

2.3 Information security principles apply to all information whatever the format or medium, including, but not limited to, hard copy and soft copy information such as manual files, handwritten notes, database, CCTV images, microfiche, speech recordings and email.

3. Roles and Responsibilities

All staff have a responsibility for ensuring information we process remains secure. Specific responsibilities for information security are set out below:

3.1 The Senior Leadership Team (SLT) are responsible for ensuring that there is an appropriate suite of policies in place that enables our compliance with relevant legislation.

3.2 The Information Governance Steering Group (IGSG) have responsibility for taking a strategic overview of information governance and information security matters and approve all policies under this framework.

3.3 The Senior Information Risk Owner (SIRO) has overall strategic responsibility for information security and this framework of policies. They have ownership of the risks associated with the information assets we hold and should act as an advocate for the organisation's information risk.

3.4 The Data Protection Officer is responsible for monitoring the council's compliance to data protection law and advising SLT and all staff of their roles and responsibilities. They assist the SIRO in assessing information risk and advise on information security matters.

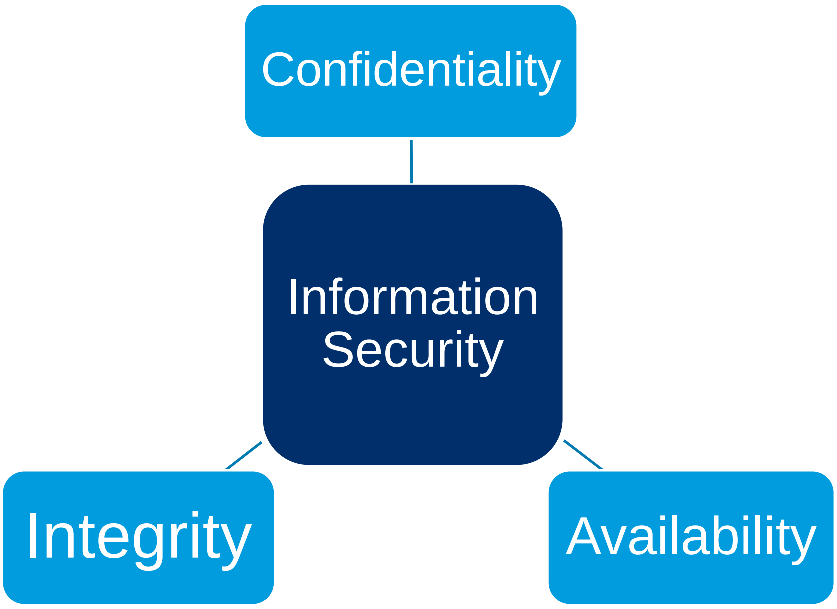
3.5 The Information Governance Team are responsible for promoting the importance of the information security throughout the organisation and providing advice and guidance on issues relating to this.

3.6 All Managers must ensure that staff receive relevant information governance and information security training, that they are aware of the Information Security Framework and suite of policies that sit within it and that their staff comply with associated procedures.

3.7 It is the individual responsibility of all Council staff, and Members, who process and manage data to ensure it is of the highest quality, secure and fit for purpose and that they comply with this policy and all others under the Information Security Framework.

4. Information Security Principles

4.1 The objective of this policy it to ensure that the fundamental principles of information security are preserved. These principles are set out in the diagram below. They are confidentiality, availability and integrity.



Confidentiality

Information Security

Integrity

Availability

4.2 The confidentiality principle of information security requires us to have measures in place to protect against unauthorised access to and disclosure of information. Having measures in place to ensure the confidentiality of information means that private information remains private and that it can only be accessed by those individuals who need that information in order to do their job.

4.3 The integrity principle requires us to have measures in place to protect information and data from unauthorised changes, alterations and deletions. This ensures that data can be trusted as accurate and that it has not been inappropriately modified.

4.4 The availability principle requires us to have measures in place to ensure the functionality of systems remains available when they are needed. The objective being that data and information is available to staff when they need it to assess a situation, make decisions and be accountable.

5. Compliance

5.1 The design, operation, use, access to and management of information systems and the information processed within those systems must be undertaken in accordance with all statutory, regulatory and contractual security requirements including, but not limited to:

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- Human Rights Act 1998
- The Health and Safety at Work Act 1974
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001

5.2 Systems and the access to them will be subject to regular risk review to ensure that we continue to comply with the information security principles to protect data.

5.3 Each information asset will have an Information Asset Owner assigned to it, who will be ultimately responsible for the security of that asset.

5.4 All new systems and processing activities will be subject to a data protection impact screening assessment and full DPIAs will be required where it has been identified that there is a risk to the rights and freedoms of data subjects (customers / staff).

5.4 The Data Protection Officer must be consulted on DPIAs and any procurement process involving new systems, this is so they can advise on matters relating to compliance.

5.6 It is the responsibility of our IT department to protect our network and keep it secure and check that there are policies and procedures in place to ensure the availability of information.

5.7 We will ensure that staff are given appropriate access to data and systems to enable them to do their jobs. There will be processes / procedures in place to approve system access.

5.8 Our buildings will be secure from physical threats and hazards in order to protect information assets contained within them. Access will be controlled appropriately throughout our offices, this may mean that some offices have greater access restrictions in place than others dependant on the risk of the information assets.

5.9 Staff will be provided with appropriate training to ensure they are able to correctly use the systems they have access to, they understand their departmental policies and procedures and that they understand and are aware of their responsibilities under data protection law.

5.10 As part of the induction process for new staff, they must undertake the mandatory information governance and information security modules on i-learn prior to access being granted to systems which hold personal and confidential information. These courses should be completed on day one.

5.11 Staff will be required to refresh their training on an annual basis.

5.12 Line managers must ensure that when a member of staff leaves their post, all leavers notifications are completed and that any IT equipment is returned and access to systems is removed.

5.13 A risk register will be in place in respect of information governance and information security matters. This risk register will be considered by the Information Governance Steering Group (IGSG) and any issues of significant concern will be escalated to the Council's Senior Leadership team.

6. Dissemination of policy

6.1 The Organisational Policy and any associated material will be initially communicated via the Council’s internal newsletters; including direct instructions that these will be discussed at all team meetings.

6.2 The Organisational Policy and any associated procedures and guidance are permanently available via the Council’s intranet.

6.3 Staff will be made aware of related policies and procedures through training and for new members of staff, through induction.

6.4 The awareness program will be renewed periodically.

7. Review of the Organisational Policy

7.1 This policy will be reviewed every 2 years by the Council’s Information Governance Steering Group (IGSG) to ensure that any national or local guidelines, standards or best practices that have been issued are considered and reflected in the policy.

7.2 All proposed amendments to the policy will be approved by the Information Governance Steering Group and Single Status Group (including Trades Unions where appropriate).