U02

Information Protection Policy

Target Audience:
User

INDEX

Section **Page**

Contents

Document Control 3
Document Amendment History 3
1 Statement of Purpose 4
2 Scope of the Policy 4
3 Storage of Information 4
4. Disclosure of Information 5
5 Compliance 6
6 Training and Staff Development Associated with Information Protection 6
7 Roles and Responsibilities 7
8 Review of the Information Protection Policy 8

Document Control

Organisation	Torbay Council
Title	Information Protection Policy
Creator	Information Security Group
Source	
Approvals	Executive Head of Information Services
Distribution	Corporate
Filename	
Owner	Information Security Group
Subject	Information Protection
Protective Marking	Unclassified
Review date	17/10/2011

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description
1	Info Security Group	17/10/11	Review
1.1	Kelly Prince	14/05/2013	Change of terms

1 Statement of Purpose

1.1 The purpose of this document is to outline the high level principles that collectively come together to form the Council's Information Protection Policy

1.2 This Information Protection Policy is a key component of Torbay Council's overall information management framework and should be considered alongside more detailed information management and security documentation including: system level security policies; Service Area specific information security guidance and protocols and procedures

1.3 It is intended that by having regard to this policy, as well as related Council wide policies and procedures, and relevant legislation the Council will facilitate not only the protection of its information during processing and transfer of information within the Council; but also compliance with relevant legislation e.g. the UK Data Protection Act, 1998

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, whether or not those assets are managed by the Council

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

2.3 Information protection 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; databases; cctv images; microfiche; speech recordings

3 Storage of Information

Information is an asset and as such must be stored in a secure and accessible manner at all times

3.1 All electronic information must be stored on the network to allow regular backups to take place.

Transient devices should be used for data in transit only.
Where users work remotely with data on local drives or any removable media, then separate policies must be complied with i.e. U08 and U09

3.2 Databases holding personal information will have a defined security and system management policy for the records and documentation. This must be agreed by Information Governance to ensure compliance with applicable legislation, e.g. the UK Data Protection Act, 1998 (COP)

3.3 Processing (including storage) of personal information must be notified to Information Governance so that the Council's Data Protection Notification can be kept up to date.

3.4 All hard copy information will be stored in accordance with any relevant guidance published by the Council

3.5 For both electronic and manual information the Council's applicable records management and retention guidance must be followed.

4. Disclosure of Information

4.1 The disclosure of information in an uncontrolled manner could pose an operational, legal and financial risk to the Council. The disclosure of personal information is strictly controlled by various legislative requirements, IG Policies and best practice guidelines

4.2 All those handling information must therefore ensure they are aware of their responsibilities when disclosing information and follow the guidance the Council has made available in relation to this, as well as any rules laid down in Torbay Councils IS framework policies

4.3 Guidance for disclosures by various means, for sharing of personal information formally using an Information Sharing Protocol and for disclosures to particular third parties such as the Inland Revenue, Police etc

4.4 If there is any suspicion users treating confidential Council information in a way that could be harmful to the Council or to the individual to whom the data refers (the data subject), then it must be reported via the methods described in the Information Security Policy.

This applies to of Council staff and Councillors; 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

5 Compliance

5.1 The design, operation, use, access to and management of information systems and the information processed within must take into consideration all statutory, regulatory and contractual security requirements

5.2 Torbay Council is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Council, who may be held personally accountable for any breaches of information security for which they may be held responsible

5.3 In order to facilitate information security, the Council shall comply with the following listed legislation and other applicable legislation as appropriate:

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

6 Training and Staff Development Associated with Information Protection

6.1 The line manger of staff will be responsible for ensuring all staff comply with the policy, and all equipment is returned when staff leave. The line manager will enforce any breaches, applying disciplinary action if required.

6.2 The Information Protection 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.

6.3 The Information Protection policy and any associated procedures and guidance will be made permanently available via the Council's intranet.

6.4 User awareness training will be made available however the line manager will ensure that all of their staff has undergone user awareness training.

6.5 All staff will be required to receive awareness training delivered by the Manager through the Induction process. Where it is recognised that staff working in certain areas of the Council need a more heightened awareness of Information Protection, additional tailored training relevant to the specific system will be given and fully evidenced by the responsible manager.

6.6 The awareness program will be renewed periodically, and during this period each member of staff will be required to retake the training.

6.7 Line managers are responsible for recovering equipment when a staff member leaves.

6.8 Line managers will complete the HR leaver's process prior to the member of staff leaving, or moves to a role requiring different access IT09.

6.9 Where relevant all new employees will have background checks undertaken on them when they start a new role, in line with HR guidance.

7 Roles and Responsibilities

Within the Council the roles and responsibility for information protection are as follows:

7.1 The Executive Head, Information Services (Chief Information Officer (CIO)) has been designated as having overall strategic responsibility for information protection

7.2 Executive Heads have both the overall responsibility for information protection within their service area, and the operational responsibility for ensuring that systems, processes and working practices enforce compliance with this Information Protection policy, and any associated and specific guidelines and procedures within their business units. They also have responsibility for monitoring and assessing compliance with the Information Protection policy and any specific related procedures within their business units

7.3 Executive Heads are responsible for reviewing the controls established, and the level of compliance with the Information Protection policy, as well as any information protection procedures and guidelines related to specific business areas

7.4 Information Governance is responsible for promoting the importance of information protection throughout the organisation and supplying advice and guidance on issues relating to this

7.5 The Executive Head, Information Services (CIO) has responsibility for ensuring that appropriate technical controls are available to enforce information protection

7.6 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. All Council staff and Members; 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 shall comply with information protection procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action

8 Review of the Information Protection Policy

8.1 This policy will be reviewed on an annual basis by Information Security Group to ensure that any national or local guidelines, standards or best practices that have been issued and that the Council needs to work to are reflected in the policy in a timely manner.

8.2 Substantive amendment to the policy will be put before the Information Governance forum for comment and adoption. Non-substantive amendments will be actioned and the revised document published in the normal course of business.

8.3 All proposed amendment to the policy will be approved by the Information Security Group