U05

Resource Protection Policy

Target Audience:
Users

Contents

Document Control

Organisation	Torbay Council
Title	U05 Resource protection Policy
Creator	Kelly Prince
Source	
Approvals	
Distribution	
Filename	
Owner	
Subject	
Protective Marking	
Review date	

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description
0.1	Kelly Prince	10/04/2011	Corporate changes
0.2	ISG	07/11/2011	First review
0.3	ISG	28/03/2011	Review
0.4	Gavin Dunphy	11/04/2012	Finalise
0.4.1	Kelly Prince	14/05/2013	Change in terms

1 Purpose

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

1.2 This Resource 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 Resource 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 Protection of facilities/sites

3.1 To protect facilities, layered physical defences must be used to protect data processing areas. Layered defences entail putting several physical barriers between the external world and the most sensitive data processing areas.

3.2 All sites must have a process for signing all visitors in. (follow up)

3.3 All sites must have procedures for controlling all keys to data processing areas.

3.4 Areas used for information processing must have separate access controls. Access controlled areas are restricted to authorised people only.

3.5 The risk to all buildings is minimised with centrally arranged contracts.

3.6 All those mentioned within the scope of this policy have responsibilities for assisting in maintaining the protection of all facilities and sites.

4 Protection of equipment

4.1 It is the responsibility of the ICT department for maintenance of all computer equipment.

4.2 When laptop computers are not being used they must be physically locked away.

4.3 Any equipment stored in public areas must be physically secured from theft using a locking cable or box.

4.4 All Data processing equipment within the main computer suite (town hall) are protected by a UPS (Uninterruptible Power Supply).

4.5 All infrastructure equipment must be secured from general access.

5 Equipment disposal

5.1 The ICT department has the responsibility for replacing all computer equipment, including all peripherals, mobile devices and storage.

5.2 All equipment waiting for, and being processed for disposal is stored in a secure location.

5.3 All IT equipment is disposed of in accordance with the WEEE directive. An accredited supplier is used for this purpose.

6 Anti-Malware Policy

6.1 The organisation employs a range of appropriate anti-malware software between the perimeter and corporate computers.

6.2 The council uses industry standard enterprise anti-virus and anti-spyware

6.3 The signatures for anti-malware software on all systems are updated daily.

6.4 On detection of an infected file the default action for anti-malware software is to quarantine the file.

6.5 The anti-malware software is set to generate full Audit Logs.

7 Device Lockdown

7.1 All Council computers will be security hardened before entering production to best practise as set out in the windows common criteria security standard. Any changes from the recommendations will be documented.

7.2 The installation of all software is the responsibility solely of the ICT department. All other users are prohibited from installing software on Authority computers.

7.3 Access to the operating system of Council computers is restricted to authorised IT administrators only, and all other users are prohibited from having administrator access to a Council computer’s operating system.

7.4 System utilities on Council computers are to be locked down from general use and are only to be used by authorised IT administrators only.

7.5 Web browsing will not be allowed to run in the context of a privileged user. Any necessary exceptions must be logged"

7.6 Council computers will not be set to a specific period of inactivity before they are automatic logged off the Council network.

8 Connection of Devices

8.1 The only processing devices allowed to be connected to Council network are Council owned devices only. All other processing devices must not be connected to the network.

8.2 Data handling devices must only be connected to the Council network in compliance with the removable media policy.

9 Protection of remote devices

9.1 Remote devices can only connect to the Council's network in compliance with the remote access policy.

9.2 All mobile devices which are used to connect to the network must be encrypted using an approved product.

9.3 The personal electronic device (PED) used within the Council are secured to the current version of the CESG security procedures. Any changes from this standard will be documented.

10 Breach procedures - compliance

10.1 Users who do not adhere to this policy will be dealt with through the Council's, or school's disciplinary process.

10.2 For Members, the Democratic Services Manager in association with the Chief Executive will ensure appropriate action is taken.

10.3 Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements.

10.4 Where the public have access to the Torbay Council system, that access will be withdrawn if there is an actual or likely breach of information security, until adequate controls are in place.

11 Review of the Resource Protection Policy

11.1 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.

11.2 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.

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