U10

Software Policy

Primary audience
Users

Contents

Document Control

Organisation	Torbay Council
Title	Software Policy
Creator	Torbay Council
Source	
Approvals	
Distribution	
Filename	
Owner	
Subject	
Protective Marking	
Review date	Year from approval

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description
Final	Torbay Council	02/07/2012	Update with ICT managers
1.1	Kelly Prince	14/05/2013	Change to 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 Software Policy

1.2 This Software 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 Software Use

3.1 Any Software shall only be used in accordance with its licence agreement.

3.2 Torbay Council holds licences for the use of a variety of software products. This software is generally owned by a software company and the copying of such software is an offence under the Copyright, Designs and Patents Act 1988

3.3 All software, systems and associated data in use for the Council is only to be used for the purposes of Council business as defined within other policies.

3.4 It is the responsibility of all Council staff to report any known software misuse to the appropriate Executive Head.

4 Software Acquisition (purchasing and or downloading)

4.1 Under no circumstances should personal or unsolicited software (this includes screen savers, games and wallpapers, etc) be loaded onto a Council machine as there is a serious risk of introducing a virus.
a) If it is necessary to load demonstration software onto a machine it must first be checked with anti virus software. Anti virus software is installed on all PC's by the ICT Department.

Laptops that have not been connected to the network must first be connected prior to downloading to ensure virus protection is up to date.

Or
b) If it is necessary to load demonstration software onto a machine it must first be approved via the ICT Service Desk, who will ensure that it is free from viruses, spyware and other malicious software.

4.2 New software may not be procured or requested unless approved by the Exec head or their nominated representative.

4.3 Any new software including third party hosted solutions may not be procured without the approval and involvement of representatives from ICT Services. This includes extensions to existing systems and or licence agreement modifications.

4.4 All software purchases and hosted solutions must be authorised via ICT Services as per financial standing orders.

4.5 The downloading and use of any open source, freeware, shareware, browser plug-ins, or other non purchased software must be approved by ICT Services (this includes applications that are supplied bundled with peripheral hardware such as digital cameras & scanners).

4.6 System controls, security and integrity of data should be considered when purchasing software from an outside supplier. Would include but not limited to:

- Contractual obligations placed on the third party in relation to data protection.
- Additional security features and tests if an application included public facing elements within it.

4.7 All new software will need to be corporately registered (in either the s/w inventory for server based apps or PCS list of supported products?)

5 Software Development and Support

(Includes MS Access, operational reports or other departmental developments being carried out beyond the confines of ICT services)

5.1 Adequate documentation and system knowledge must be present to enable systems to be supported and maintained effectively. Consideration must be given to what would happen if the original architect is not available.

5.2 All systems should have built in security, which restricts access to sensitive data to authorised persons only. Data entry screens should have validation controls to reduce the risk of invalid data being added or existing data being corrupted.

If in any doubt, Individual's developing solutions, should contact Information Governance to answer questions about "sensitivity" and discuss with ICT Services potential options for ensuring adequate security. Password protecting a file will not be considered robust enough in certain circumstances.

5.3 All new systems will need to be corporately recorded. (does not include modifications to existing systems)

6 Installing Software

6.1 Software must only be installed by the ICT Department unless otherwise agreed by the Exec Head of Information Services. A register of individuals outside of ICT who are allowed to install s/w is to be maintained by ICT services.

6.2 It is the responsibility of installer to ensure that all the software is correctly licensed.

6.3 It is the responsibility of the installer to ensure that appropriate backup's of data will be made and that a recovery from the backup is performed as a test. This involves contacting ICT to ensure that backups are put in place.

7 Critical Systems Change Management – As defined in the Councils Corporate Business Continuity plan

7.1 There must be a designated senior user who is responsible for authorising and accepting changes to the system. Provision must be made so that modifications are fully tested in a test environment. Software can only go live with senior user authorisation.

7.2 ICT will apply formal change control procedures when undertaking system modifications. This should be applied to all systems under this heading unless in the case of emergency changes. In such circumstances retrospective approval for the change must be sought.

7.3 There are isolated occasions where the ICT Services are requested to update operational data. This should be supported by a written request from the owner of that data, which details the changes required. If possible the change should be applied to the test system prior to the designated senior user approving the live change.

7.4 Any Individual or 3rd party having the software tools that provide direct access to live data with update rights needs to be registered with the Software Development Manager. Any such privileges are to be reviewed on a regular basis by the SDM.

Access by third parties is governed by corporate policy.

7.5 ICT Services will maintain a change history which will document the nature of the change, who approved the change, who and how it was tested and who approved it to go live.

8 Review of the Software 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