U04
Third Party Use of Resources Policy

Target Audience:
Partner

INDEX

Section **Page**

Contents

Document Control

Organisation	Torbay Council
Title	Third Party Use of Resources Policy
Creator	Information Security Group
Source	
Approvals	Executive Head of Information Services
Distribution	Corporate
Filename	
Owner	Information Security Group
Subject	Information Security Responsibility
Protective Marking	Unclassified
Review date	09/11/2011

Document Amendment History

Revision No.	Originator of change	Date of change	Change Description
1	Info Security Group	09/11/2011	Review
2	Gavin Dunphy	19/10/2015	Added guidance around sharing access to council managed devices with a third party

1 Statement of Purpose

1.1 The purpose of this document is to outline the high level principles that collectively come together to form Torbay Council's Third Party Use of Council Resources Policy and formalise how information technology and associated equipment should be used by individuals employed by external agencies working for Torbay Council

1.2 This policy is a key component of Torbay Council's overall information and security 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 where applicable

1.3 It is intended that by having regard to this policy, as well as related Council wide policies and procedures, and relevant legislation, Torbay Council will facilitate the management and security of information in all its forms

2 Scope of the Policy

2.1 This policy applies to all 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 Computer equipment, software, data access and services provided by Torbay Council for use in conducting Council business is supplied on the following terms and conditions:

3 General

3.1 These Conditions of Use may be modified from time to time, in response to changing circumstances of an operational, legislative or technological nature

3.2 Periodic checks may be made by designated Council staff to ensure compliance with these conditions.

4 Ownership

4.1 The computer equipment, software, data access and services provided are the property of Torbay Council. The equipment shall be recorded in the inventory of IT equipment and software, which is maintained by IT Services. They are provided for the duration of your work with the Authority

4.2 At the end of that period services provided will be terminated and computer equipment, software, removable media and data must be returned to the Council. (IT11 Leavers form)

5 Installation

5.1 The equipment, software and services will be prepared for your use by an officer of Torbay Council in accordance with the correct council policy and relevant current legislation.

5.2 Torbay Council will be responsible for supplying the equipment and any leads necessary to operate the equipment

6 Use of Computer Equipment, Software and Services

6.1 The equipment, software and services are provided for use in respect of Torbay Council business. In making use of the facilities provided you are required to comply with the Council's policy and guidelines with respect to the use of Information Communications Technology. These include, but are not limited to:

6.1.1 Financial Regulations
6.1.2 DISP Framework

6.2 The relevant policies will have been supplied to you, and are available on the Council's intranet.

6.3 Torbay Council accepts no liability for any consequences (including financial or other loss) which may arise through any private use of the facilities provided

6.3.1 You should only use the facilities for private use in line with applicable policies

6.3.2 You should also note that the security of private information and data whilst using the provided facilities is your responsibility and may be monitored

6.3.3 You are advised that if you generate private information on Council hardware simply deleting files does not permanently remove them from a computer

6.4 Access to the Internet may be provided by the Council. You should be aware that the Internet contains potentially offensive material (refer to Section 10)

6.5 Torbay Council accepts no liability for any offence, injury or consequences that may result from your use of the equipment and its associated facilities.

6.6 You are reminded of your responsibility of probity (see Section 11).

7 Computer Security

7.1 Torbay Council's Security Policy must be complied with at all times

7.2 In addition, the following basic criteria must be adhered to:

7.2.1 Information concerning Torbay Council's computer security arrangements and access methodologies must not be divulged to unauthorised persons

7.2.2 The use of all media (e.g. floppy disks, CDs, Memory Sticks) must be in line with removable media policy

7.2.3 Where a virus is suspected/detected, the matter must be reported to IT Helpdesk immediately. Until virus repair is affected, an infected PC must not be used

7.2.4 Virus repair must be undertaken only by or under the guidance of staff of ICT

7.2.5 No software can be loaded onto the Council's ICT equipment, except by authorised departments/ users such as PC Support and IT Services

7.2.6 All data must be stored or backed up on the Torbay Council network drive.

7.2.7 Where information is kept on portable media, such as USB sticks, then such media must be kept securely when not in use

7.2.10 Where lost/stolen equipment and/or software are recovered; or where it is suspected that equipment or software have been tampered with, they must returned to ICT for testing prior to re-use

7.2.11 When using Council owned equipment, you must not store/save any data on external hosted sites other than those owned/approved by Torbay Council.

8 Risk Management and Insurance

8.1 As part of its risk management and risk financing arrangements, the Council maintains insurance on the equipment provided to you, including cover against the perils of theft, accidental damage, malicious damage and fire

8.2 All computer equipment must be secured from theft or unauthorised use as far as is practical

8.3 If you travel with a laptop or other equipment, it should not be left in an unattended vehicle unless there is no other option, in which case it should be secured out of sight in the boot. There is no insurance cover for losses arising from unlocked vehicles, hotel rooms or other unsecured situations. Therefore, you should be especially careful when taking a laptop away from Council offices, as you will be liable for any such loss

8.4 Any loss of, or damage to, the equipment and data should be reported immediately to your service area manager, IG, Internal Audit and Corporate Security

9 Internet Access and Electronic Mail

9.1 Any third party internet access and electronic email use must be in accordance with the relevant policies within the Security Policy – Email and Internet, and third party users must be aware of their DP obligations

10 Probity

10.1 All officers and members are bound by the National Code of Local Government Conduct and the general principles contained within the Code also apply to specific instances, such as the use of the Internet, Intranet or e-mail. All other individuals who work on behalf of the council will be expected to act in a manner that complies with these codes, therefore you

should ensure that your conduct accords with the requirements of the National Code and that of Torbay Council's Code of Conduct

10.2 All officers and members are bound by the Fraud and Corruption policy. All other individuals who work on behalf of the Council will be expected to act in a manner that complies with this policy, therefore you should ensure that you are aware of the requirements of the policy.

10.3 Any allegations of breach of the Codes will be dealt with through means of the Whistleblowing procedure

11 Support

11.1 Any computer equipment, software or data related problems which occur should be reported to IT Service desk and Information Governance if data related during normal working hours, quoting the asset number from the yellow label attached to your PC. This will ensure that the problem is tracked and concluded as quickly as possible

11.2 No support will usually be provided outside of normal working hours

11.3 In the event that the equipment suffers a complete hardware malfunction, Torbay Council will be responsible for putting the equipment back to the condition in which it was first supplied. The Council will also reinstate, in so far as is reasonable and possible, information and data secured from the most recent back-up

12 Health and Safety

12.1 Link to H&S policies on the intranet and the need for third party DSE assessments.

13 Information / Data Use

13.1 Any information and/ or data that is available to be accessed must only be used for the Council's purposes and all processing must comply with applicable legislative requirements and Torbay Council's policies, guidelines and procedures, and in particular must not be transferred to any third party or other employers without the explicit written agreement of the relevant service area manager and only following the advice of Information Governance.

14 Compliance

14.1 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

14.2 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

14.3 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

15 Training and Staff Development Associated with Third Party Use of Resources

15.1 The line manger of any third party using Council resources will be responsible for ensuring all third parties comply with the policy, and all equipment is returned by the third party. The line manager will respond to any breaches, applying contract / service agreement conditions action if required.

15.2 The line manager will be responsible for ensuring that the third parties have signed acceptance of the Information security policy.

15.3 The Third Party Use of Council Resources 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.

15.4 The Third Party Use of Council Resources Policy and any associated procedures and guidance will be made permanently available via the Council's intranet.

15.5 User awareness training will be made available; however the line manager will ensure that all of their third parties using Council resources have undergone user awareness training.

15.6 All third parties using Council resources will be required to receive awareness training delivered by the Manager. Where it is recognised that third parties working in certain areas of the Council need a more heightened awareness of information security, additional tailored training relevant to the specific system will be given and fully evidenced by the responsible manager.

15.7 The awareness program will be renewed as and when needed, and during this period each third party using Council resources will be required to retake the training.

15.8 Line managers will be supplied a checklist of equipment to recover when a third party leaves.

15.9 Line managers will inform IT Services in advance of the third party leaving or moving to a role requiring different access rights.

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

16 Shared access of Computer Equipment, Software and Services

16.1 There are times when it is necessary to allow a 3rd party to take control of a managed device under a users own credentials (e.g., in order that the 3rd party can remotely support particular software on the device).

16.2 The 3rd party must never be provided with credentials – the individual sharing access must always enter credentials in advance of providing access to the 3rd party.

16.3 The 3rd party must never witness the credentials being entered.

16.4 The individual providing credentials must have complete oversight of any action carried out by the 3rd party. Should that individual need to lose oversight even for a brief period they must first log off and/or take back exclusive control of the device before doing so.

16.5 The individual providing credentials must ensure that only relevant information is accessible on the managed device. Unrelated documents and applications (e.g. email) must be closed before handing over control to prevent accidental disclosure of information.

16.6 The individual providing credentials will be held responsible for any loss of confidentiality, integrity or availability resulting from their providing access to a 3rd party.

17 Roles and Responsibilities

17.1 It is managers' responsibility to ensure that all staff are aware of relevant policies to their role.

17.2 It is the responsibility of all those provided with an individual email account to manage their account in accordance with this Policy and in accordance with direction from the Executive Head Information Services (CIO). Failure to comply may lead to legal action, withdrawal of use and disciplinary action that could result in dismissal.

17.3 It is the responsibility of managers within directorates to exercise appropriate controls to minimise the risk of misuse. Where misuse is suspected or found advice should be sought from the Council's Internal Auditors, Human resources and the Information Security Incident Policy must be followed.

17.4 The decision over email suitability for sending each email message is the responsibility of the individual sender.

18 Review of the Third party use of resources Policy

18.1 This policy will be reviewed on an annual basis by Information Governance 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.

18.2 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.

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