###


###

 U03

 Access Control Policy

This document is copyright to Torbay Council and should not be used or adapted for any purpose without the agreement of the Council.

|  |
| --- |
| Target Audience: |
| **Manager & ICT** |

**Contents**

[Document Control 3](#_Toc308082949)

[Document Amendment History 3](#_Toc308082950)

[1 Statement of Purpose 4](#_Toc308082951)

[2 Scope of the policy 4](#_Toc308082952)

[3 User Access Management 4](#_Toc308082953)

[4 New network accounts 4](#_Toc308082954)

[5 Account removal 5](#_Toc308082955)

[6 System / Application Accounts 5](#_Toc308082956)

[7 Network Administrator Accounts 5](#_Toc308082957)

[8 Generic accounts 6](#_Toc308082958)

[9 Service Account 6](#_Toc308082959)

[10 Account Review 7](#_Toc308082960)

[11 Account Authentication 7](#_Toc308082961)

[12 Two-factor authentication (RSA) 7](#_Toc308082962)

[13 Compliance 7](#_Toc308082963)

[14 Training and Staff Development Associated with Access Control 8](#_Toc308082964)

[15 Roles and Responsibilities 8](#_Toc308082965)

[16 Review of the Access Control Policy 9](#_Toc308082966)

# Document Control

|  |  |
| --- | --- |
| **Organisation** | Torbay Council |
| **Title** | Access Control Policy |
| **Creator** | Gavin Dunphy |
| **Source** |  |
| **Approvals** | Executive Head of Information Services |
| **Distribution** | Corporate |
| **Filename** |  |
| **Owner** | Information Security Group |
| **Subject** | Employee Access Control |
| **Protective Marking** | NOT PROTECTIVELY MARKED |
| **Review date** | 17th October 2011 |

# Document Amendment History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision No.** | **Originator of change** | **Date of change** | **Change Description** |
| 0.1 | Karen Mitchell |  | Document creation. |
| 0.2 | Gavin Dunphy |  | Responsibility taken over by networks |
| 0.3 | Gavin Dunphy |  |  Integration of Template and v0.2 |
| 0.4 | Information Security Group | 17/10/2011 | Review |
| 0.5 | Gavin Dunphy | 01/11/11 | Review Generic & Shared accounts |
| 0.6 | Audit / ICT | 10/11/11 | Review Generic accounts |
| 0.6.1 | Kelly Prince | 14/05/2013 | Change of terms |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 1 Statement of Purpose

* + 1. Information is a major asset that Torbay Council has a duty and responsibility to protect.

1.2 The purpose and objective of this Access Control Policy is to specify the means of controlling access to Council’s Computer network, systems and data therein.

## 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 User Access Management

3.1 Every user of the Torbay Council network must have a network account

3.2 Network users who have multiple roles will be required to have a unique network account for each distinct role.

3.3 Each network account will be set to disable access to the network after a set number of failed log on attempts.

3.4 Standard network user accounts must not be shared between members of staff. Unauthorised sharing of network user accounts will be considered a contravention of this policy and will be dealt with accordingly.

## 4 New network accounts

4.1 Torbay Council exercises a formal user registration and deregistration process for all network users, permanent and temporary.

4.2 The privileges applied to any accounts must be the minimum required for the role.

4.3 All new accounts are to be requested and authorised by an appropriate line manager before the employee starts using the appropriate IT form with all of the required access specified.

4.4 New accounts are created with a password which the user is required to change at first logon.

4.5 The initial password for a user account will only be given to the new user via the standard notification letter

4.6 Users must keep their password secure and known only to themselves.

4.7 Sharing of passwords is not permitted as per 3.4.

## 5 Account removal

5.1 All network accounts for a member of staff will be disabled if that member of staff leaves the council on receipt of an appropriate IT form. The account is deleted on formal confirmation from HR via their Starters & Leavers process.

5.2 Notification of leavers (both internal and external) must be provided to Human resources via an appropriate IT [form](https://secure.torbay.gov.uk/ITForms/) a minimum of 5 working days before departure by the employee’s service manager. This will be actioned on the leaving data i.e. disabled.

5.3 Accounts used by staff on long term absence will be disabled, unless specified as required by the line manager.

## 6 System / Application Accounts

6.1 System Administrators are responsible for managing separate logon accounts for their own systems, setting permissions and monitoring account usage.

## 7 Network Administrator Accounts

7.1 These are defined as accounts created for individual users within IT Services with network administration roles

.

7.2 Authorisation is required from the IT service manager to create Administration accounts

7.3 All administrator accounts must be identifiable and used only for administration purposes

7.4 All Administrator accounts must be separate from user accounts

7.5 Network System Administrators are responsible for managing separate logon accounts for their own systems, setting permissions and monitoring account usage

7.6 All activities of network administrator accounts will have audit logs enabled, giving a full audit trail of actions

7.7 Standard network accounts will not routinely have network or computer administrative access unless there is an authorised business need.

## 8 Generic accounts

8.1 This is defined as an account that does not contain the specific name of an employee, may be used by one or more staff

8.2 The use of generic accounts is permitted only with a valid business case and agreed by ICT and is in compliance with government guidelines

8.3 A generic account will not be a substitute for a named account (including temporary staff), but will be allowed to provide access for specific roles to perform specific functions.

8.4 Each generic account will have an officer named as the responsible person. A secondary officer must be named for business continuity purposes and the responsible officer must be given full delegated access to any mailbox associated with the account

8.5 The privileges applied to generic accounts must be only the minimum required for the role

8.6 On commencement of use of the account the responsible person, see 8.4, must ensure that a suitable procedure is in place to identify the user of the generic account

8.7 Type of generic accounts should be limited to the minimum required. In order of preference, these types are:

* + Local User Account
	+ Local Admin Account
	+ Domain User Account
	+ Domain Admin Account

8.8 All usage will be logged and will be available for audit control

8.9 Once setup Generic accounts will be subject to ICT usage control and review

8.10 Email will be disabled for generic accounts unless there is a valid business case. Remote email access will be disabled in all cases, ensuring that if there is a failure in password reset procedures, access cannot be gained to the account by someone who has left the Council

8.11 Internet access will be disabled for generic accounts unless there is a valid business case

## 9 Service Account

9.1 Service accounts are accounts which are not used by individuals but by applications to run services

9.2 Service accounts must be authorised by the Executive Head, Information Services

9.3 Interactive logon must be disabled for service accounts

9.4 Password for service accounts are the responsibility of the Administrator and must be stored and recorded securely

## 10 Account Review

10.1 Network Accounts that have not been used for 90 days will be automatically disabled

10.2 Unused network accounts that have been disabled for 90 days will be deleted on verification of the account

10.3 System / application accounts will be disabled in line with system / application settings.

## 11 Account Authentication

11.1 Strong password controls are established.

11.2 Passwords for network accounts must not be shared unless an authorised shared account (is this somewhere else? Link to 4.7) (check)

## 12 Two-factor authentication (RSA)

12.1 Two-factor authentication refers to authentication dependent on something the user knows (some form of password) plus something the user has (some physical device)

12.2 Two-factor authentication will be employed for all remote access

12.3 Two-factor authentication devices will be allocated and managed centrally

12.4 Two-factor authentication devices must not be shared with anyone

12.5 The loss of a two-factor device must be reported immediately according to the Information Security incident reporting [procedure](http://insight/index/information/informationgovernance/data_security_breaches.htm)

12.6 The “known” part of the authentication must not be physically recorded anywhere

## 13 Compliance

13.1 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

13.2 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

13.3 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

## 14 Training and Staff Development Associated with Access Control

14.1 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.

14.2 The Access Control 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.

14.3 The Access Control policy and any associated procedures and guidance will be made permanently available via the Council’s intranet.

14.4 User awareness training is available however the line manager will ensure that all of their staff has undergone user awareness training.

14.5 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 Access Control policy, additional tailored training relevant to the specific system will be given and fully evidenced by the responsible manager.

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

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

14.8 Line managers will complete the HR leaver’s [process](https://secure.torbay.gov.uk/ITForms/#/Home) prior to the staff member leaving or moves to a role requiring different access rights ([IT09](https://secure.torbay.gov.uk/ITForms/#/Home))

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

## 15 Roles and Responsibilities

Within the Council the roles and responsibility for employee IT access are as follows:

15.1 The Executive Head, Information Services (Chief Information Officer (CIO)) has been designated as having overall strategic responsibility for access controls.

15.2 Executive Heads have both the overall responsibility for access controls within their service area, and the operational responsibility for ensuring that systems, processes and working practices enforce compliance with this Access control policy, and any associated and specific guidelines and procedures within their business units. They also have responsibility for monitoring and assessing compliance with the Access Control policy and any specific related procedures within their business units

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

15.4 Information Governance is responsible for promoting the importance of access control throughout the organisation and supplying advice and guidance on issues relating to this

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

15.6 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 access control procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action

## 16 Review of the Access Control Policy

16.1 This policy will be reviewed on an annual basis by the 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.

16.2 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.

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