Torfaen County Borough Council

Acceptable Use Policy

Version 4.0 Live

**DOCUMENT CONTROL**

|  |  |  |  |
| --- | --- | --- | --- |
| **Title:** | **Acceptable Use Policy** | | |
| **Document Owner:** | **Senior Information Risk Owner** (SIRO) | | |
| **Document Author:** | **Sharon Clifford** | | |
| **Reference:** | **IG006** | **Retention Period:** | **Until next review** |
| **Document Classification:** | Official | **Location:** | SWOOP |
| **Version / Status:** | 4.0 Live | **Approved by:** | SIRO/Leadership |
| **Current Issue Date:** | January 2022 | **Next Review Date:** | January 2025 |

**REVISION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue Date** | **Version / Status** | **Reason for Change** | **Changed By:** |
| April 2018 | 1.0 Live | Policy Implementation/changes | Sue Bullock |
| October 2019 | 2.0 Live | Minor grammatical corrections | Leah Hardwick |
| August 2020 | 3.0 Live | Updated to include new ways of working and Appendix removed to form separate guidance | Sharon Clifford |
| January 2022 | 4.0 Live | Template updated to coincide with Procedure update/review. Minor changes to Sections 1 and 2 referencing personal devices | Sharon Clifford |
|  |  |  |  |

**Table of Contents**

[**1.** **PURPOSE** 4](#_Toc89781475)

[**2.** **SCOPE** 5](#_Toc89781476)

[**3.** **AIMS & OBJECTIVES** 5](#_Toc89781477)

[**4.** **RESPONSIBILITIES** 6](#_Toc89781478)

[**5.** **LEGISLATION & KEY REFERENCE DOCUMENTS** 7](#_Toc89781479)

[**6.** **MONITORING AND REVIEW** 8](#_Toc89781480)

[**7.** **COMPLIANCE** 8](#_Toc89781481)

# **PURPOSE**

The Purpose of the Acceptable Use Policy is to:

* Outline the acceptable use of all ICT equipment owned by Torfaen County Borough Council and also includes personal devices authorised via Bring Your Own Device (BYOD) when accessing corporate information.
* Set out the parameters, boundaries and conditions of workplace and personal use to protect the interest of both the Council and users.
* Explain what the Council deems as acceptable use of information systems/services and to minimise the risks associated with accidental or malicious abuse of any equipment, information, and associated services.
* Make clear that the use of the Council’s equipment and systems are for Council business use and where allowed, any personal usage **must not** interfere with an individual’s work activity and responsibilities.
* Advise and protect both the employee/user and the Council as inappropriate use exposes the Council to risks including virus attacks, the compromising of network systems and services, and legal issues to which non-compliance could lead to a disciplinary investigation against the user.
* Ensure that in circumstances where a Council employee/user or worker is utilising the equipment or systems of another organisation within the course of their employment, this policy is supplemented by the provisions and restrictions set out by that organisation. Those employees are expected to obtain copies of any relevant IT/ equipment usage policies either directly or through their line manager and apply these when using those systems and equipment owned/loaned by the organisation

# **SCOPE**

This policy applies to:

* All employees, whether office based or working via remote access, including contractors, volunteers, agencies and partner organisations operating on behalf of the council.
* All elected members whilst working on council business.
* All equipment that is owned or leased by the Council.
* All resources owned by the Council including corporate information which is held/accessible on personal devices approved through BYOD

# **AIMS & OBJECTIVES**

This Policy aims to establish acceptable working practices to protect the Council and those users carrying out work on its behalf which will:

* Ensure that all members of staff/elected members and third-party users are aware of and understand their personal responsibilities in the acceptable/non-acceptable use of corporate information and systems/applications controlled by the Council.
* Provide a clear Acceptable/Non-acceptable Procedure document to support this policy which is available to all users.
* Ensure the confidentiality, integrity and availability of information and systems are adequately protected.
* Enable staff/elected members and all third-party users to utilise the information, equipment and networks appropriately and thereby ensure the Council is not compromised through inappropriate use as set out in the Acceptable Use Procedure.
* Support, advise and protect staff/elected members and all third-party users from non-compliance and potential disciplinary action.

# **RESPONSIBILITIES**

The following individuals/groups have specific responsibilities:

|  |  |
| --- | --- |
| Senior Information Risk Owner (SIRO) | Overall executive responsibility for the Acceptable Use Policy (Procedure and standards) and their application throughout the Council |
| Data Protection Officer | To monitor and promote compliance of the Acceptable Use Policy and Procedure and report back to the service areas via Leadership Team and the IMG  Review, implementation, and governance through the Information Asset Owner’s Group (IAOG) and Information Management Group (IMG) |
| Data Protection and Information Governance Team | Policy formulation and review and providing advice and guidance  Ensuring that the Acceptable Use Policy and Procedure are kept up to date and relevant to the needs and obligations of the Council |
| Heads of Service/Line Managers | Ensuring that this Policy and the Procedural document are made known to all staff, inclusive of agency workers, contractors, volunteers, students or anyone accessing the Council’s systems or information and in doing so ensuring awareness of their responsibilities for acceptable use/actions  To assign clear responsibility for information which passes out of their control following (for example) restructuring, moving of functions, closing of projects |
| All staff and elected members | Adherence to the Acceptable Use Policy and Procedure and related standards/guidance when managing, storing and disposing of the information they create and receive during the course of their duties  To undertake any training/awareness provided  To ensure that the information held by the Council is disposed of appropriately and that all sensitive information is disposed of securely  To report immediately any observed or suspected incidents where sensitive information has or may have been insecurely disposed of  Documenting of processes and evaluating procedures within their service areas |
| Systems Administrators | Management of the data systems in their service area in conjunction with SRS technical staff. System-specific procedures should be made available to all staff using specialised service area systems such as (but not limited to) WCCIS/Civica/etc. |
| Shared Resource Service (SRS) | Managing the network infrastructure, ensuring system continuity and security |

# **LEGISLATION & KEY REFERENCE DOCUMENTS**

**(Please note this list is not exhaustive)**

The Council will abide by all relevant UK and EU legislation and the following policies and procedures:

* The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
* The Data Protection Act (2018)/The Data Protection Bill
* The Copyright, Designs and patents Act (1988)
* The Computer Misuse Act (1990) / (2011)
* The Health and Safety at Work Act (1974)
* Human Rights Act (1998)
* Regulation of Investigatory Powers Act 2000
* Freedom of Information Act 2000
* Environmental Information Regulations 2004
* Social Services & Well-being (Wales) Act 2014
* Children Act 2004 / 2019
* Equality Act 2010
* Crime and Disorder Act 1998
* Privacy and Electronic Communications (EC Directive) Regulations 2003 (amended 2019) PECR
* Welsh Language Standards

###### **TCBC POLICIES**

* Data Protection Policy
* Information Governance Framework
* Information Governance Policy
* Information Security Policy
* Information Sharing Policy
* Records Management Policy
* Retention Policy
* Information Secure Destruction Policy
* Information Access Policy
* Information/Data Loss Policy
* Requests for Information Policy
* Clear Desk Policy
* FOI Policy
* Password Policy
* BYOD Policy
* Social Media Policy
* Dignity at Work Policy

###### **TCBC PROCEDURES**

* Data Protection Procedures
* Off Site Archive & Destruction
* Password Construction Procedures
* Retention Schedule (on SWOOP)
* Acceptable Use Procedures
* BYOD Guidance
* Social Media Guidance
* Disciplinary Rules and Procedures
* Code of Conduct for Employees

# **MONITORING AND REVIEW**

The Information Management Groups are responsible for reviewing the content and ensuring that policies are published on the Information Management site on SWOOP. This Policy will be subject to review when any of the following conditions are met:

###### Content errors or omissions are highlighted.

###### Where another standard/guidance issued conflicts with the information in this policy.

###### An initial 1 year review from policy implementation and on a 3 yearly basis from the current version approval date.

# **COMPLIANCE**

Failure to comply with this policy may be regarded as misconduct and investigated under the Council’s Disciplinary Rules and Procedures.  In serious cases this may be considered gross misconduct and lead to dismissal from the Council’s employment without notice or payment in lieu of notice.  In serious cases individuals may be liable for prosecution under Data Protection Law