Information Security Policy

V1.12

t

Issue Date	Version	History of Changes	Approval
08/06/09	1.0	Approved	ICT Security Forum
22/07/09	1.1	Approved	Full Council
22/07/10	1.2	Approved	ICT Security Forum
08/12/10	1.3	Approved	Full Council
12/12/11	1.3	Approved	ICT Security Forum
Dec 2012	1.3	Approved	ICT Security Forum
12/12/13	1.3	No changes made. Approved for publication.	ICT Security Forum
25/02/2014	1.3	No policy changes.	ICT Security Forum.
05/08/2014	1.4	Responsibilities updated to reflect IGF responsibilities.	Information Governance Forum.
05/02/2015	1.5	Statement added to the policy in relation to continual improvement.	Information Governance Forum.
05/02/2016	1.6	Update to reflect acceptance and adherence by nonnetwork users.	Information Governance Forum.
11/03/2016	1.7	Updates made to Disposal of ICT Equipment Policy; Email AUP; Internet AUP; Remote working Policy; Unauthorised Access Policy.	Information Governance Forum
16/03/2017	1.8	Social Media Policy added to Supporting Operational Policies; Responsibilities updated in regard to third parties.	Information Governance Forum
06/02/2018	1.9	CCTV Policy and Members Social Media Policy added to Supporting Operational Policies.	Information Governance Forum
27/09/2018	1.10	Supporting operational policy amendments – Data Protection Policy replaced with Privacy Standards Policy and Data Protection Breach Policy added. DPO responsibilities added.	Information Governance Forum (IGF)
18/10/2019	1.11	No policy updates – Approved	IGF
27/01/2021	1.11	No policy updates – Approved	IGF
17/11/2021	1.12	Strengthened training statement in relation to mandatory training	IGF
25/11/2022	1.12	No policy updated – Approved	IGF
25/01/2024	1.12	No policy updates – Approved	IGF

Definition of Information Security

Information is an important business asset to Merthyr Tydfil County Borough Council (MTCBC); it is essential to the organisations business need. The protection of information has become more important due to increasing interconnectivity, as it is now exposed to a wider variety of threats and vulnerabilities.

Information can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, it should always be appropriately protected.

Information Security is the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk and maximise business opportunities.

Information Security is achieved by implementing a suitable set of controls, including policies, processes and procedures, organisational structures and software and hardware functions.

Objective

The objective of the Information Security Policy is to protect the information assets processed by MTCBC from all appropriate threats. Compliance with the Information Security Policy is necessary to ensure business continuity and minimise business damage by preventing the occurrence of and minimising the impact of information security incidents.

This policy will support the organisation in its operations of ICT and Information Security whose aim is to maintain:

Confidentiality of information: protecting access to it.

Integrity of information: preventing alteration of information.

Availability of information: ensuring information and services are available to authorised persons when required.

This policy will help to minimise the risks, from whatever source to the security of ICT facilities and intends introducing appropriate levels of controls to offer adequate protection without unnecessary expense or intrusion.

Scope

The policy applies to:

- All MTCBC employees and school-based staff engaged in work for MTCBC, including working from home or non MTCBC locations.
- Other persons working for MTCBC, whilst engaged on MTCBC business or using MTCBC equipment and networks (including wireless).
- Members of the Authority when using MTCBC equipment or using MTCBC networks (including wireless).

Information takes many forms. The scope of the Information Security Policy includes, but is not limited to information which is:

- Stored on computers.
- Transmitted across networks.
- Printed out.
- Written on paper.
- Sent by fax.
- Stored on tapes, disks, USB memory sticks or any other removable media.
- Spoken in conversation e.g., by telephone or video call/meeting.
- Sent via email.
- Stored on databases.

Various operational policies and procedures support this Information Security Policy.

Responsibilities

The Chief Executive shall be accountable for ensuring that appropriate security and legal controls are identified, implemented and maintained. The Chief Executive shall be supported in this task by all employees.

The Senior Information Risk Owner (SIRO) is responsible to ensure organisational information risk is properly identified and managed and that appropriate assurance mechanisms exist.

All employees, Members, third parties and school-based staff will be asked to read, familiarise and ensure they have understood this Information Security Policy (and all supporting operational policies that are relevant to them) and their role and responsibilities in complying with it.

The role and responsibility for managing information security at an operational level shall be performed by the Corporate Information Security Officer.

It is the responsibility of all employees, Members, third parties and school-based staff to adhere to the Information Security Policy and supporting operational policies.

Non-compliance of the Information Security Policy and supporting operational policies by any employee shall result in disciplinary action, Members will be in breach of the Members Code of Conduct, and a case will be presented to school governors to consider disciplinary action against school-based staff. In the case of third parties, an investigation report will be presented to their organisation and their access to MTCBC information assets and/or network may be suspended.

In order to support the goals and principles of information security in line with business strategy and objectives, the ICT department has a positive commitment to improve communications with other departments and key suppliers to help support and implement the goals and objectives of this security policy.

MTCBC recognises Information Security as an enabler to electronic services delivery and sharing of information with the Council's partners.

The organisation is committed to continually improving its information security management system by performing audits, reviews, and measurements, by managing incidents and risks, setting objectives, monitoring performance, evaluating results and implementing corrective actions.

The Data Protection Officer will monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

The Information Governance Forum are authorised to update and amend the Information Security Policy and the supporting operational policies following consultation with the Portfolio Member for Business and Regulatory Services.

Policy Statements

The Information Security Policy provides that Merthyr Tydfil County Borough Council shall ensure that:

- Information assets and information processing facilities shall be protected.
- Confidentiality of information assets shall be a high priority.
- Integrity of information shall be maintained.
- MTCBC's requirements, as identified by information owners, for the availability of information assets and information processing facilities required for operational activities shall be met.
- Statutory, and expressed implied legal obligations shall be met.

- Business continuity plans shall be produced, maintained and exercised.
- Unauthorised use of information assets and information processing facilities shall be prohibited; the use of obscene, racist or otherwise offensive statements may lead to disciplinary action.
- Controls shall be commensurate with the risks faced by MTCBC.

Training

It is a condition of having an account on MTCBC's network that all employees, Members and school-based staff shall complete all relevant Information Security awareness training, in order to minimise the risk of a security incident or breach. Those staff and Members that do not complete training within the specified 12-month period, will have their network accounts disabled and may be subject to disciplinary action.

Policy Acceptance

Agreement to the Information Security Policy, also confirms agreement and adherence to the following supporting operational policies for staff, Members and school-based staff that have a computer account on the network (available on the Intranet or from the Information Security Officer):

- Antivirus Policy
- CCTV Policy
- Clear Desk Policy
- Privacy Standards Policy
- Disposal of ICT Equipment Policy
- Email Acceptable Use Policy
- ICT Procurement Policy
- Information/Asset Protection Policy
- Information Backup and Storage Policy
- Internet Acceptable Use Policy
- Password Policy
- Physical Security Policy
- Remote Working Policy
- Removable Media Policy

- Reporting Information Security Events Policy
- Social Media Policy (for employees)
- Members Social Media Policy (for Members)
- Software Compliance Acceptable Use Policy
- Telephones and Facsimiles Policy
- Unauthorised Access Policy
- Legal Responsibilities in Relation to Information Security
- Data Protection Breach Policy

Policy Acceptance for Staff without a Computer Account

Agreement to the Information Security Policy, also confirms agreement and adherence to the following supporting operational policies for those staff and school-based staff that do not have a computer account on the network (available from Human Resources, your Manager or from the Information Security Officer):

- CCTV Policy
- Clear Desk Policy
- Data Protection Policy
- Disposal of ICT Equipment Policy
- Information/Asset Protection Policy
- Physical Security Policy
- Reporting Information Security Events Policy
- Social Media Policy (for employees)
- Telephones and Facsimiles Policy
- Unauthorised Access Policy
- Legal Responsibilities in Relation to Information Security
- Remote Working Policy.

Policy Review and Maintenance

The Information Security Policy shall be reviewed annually and at other times as dictated by operational needs.

Confirmation of Acceptance & Adherence

I confirm my acceptance and adherence to the Information Security Policy **v1.12**,
I confirm I have read and understood the contents of the policy.

Print **Full** Name: _____

Job Title: _____

Signature: _____

Date: ____ / ____ / _____