IT Policy

Ensuring Responsible Use and Security of Information Technology Resources

Introduction

This IT policy outlines the acceptable use, security measures, and responsibilities concerning the organisation's information technology resources. It is designed to safeguard the organisation's digital assets, ensure compliance with legal and regulatory standards, and promote responsible use of technology by all employees, contractors, and stakeholders.

Scope

This policy applies to all councillors, employees, contractors, and any users who access the council's IT resources, including but not limited to computers, networks, software, data storage systems, website, email, mobile phones and messaging apps.

Objectives

The objectives of this policy are:

- To ensure the confidentiality, integrity, and availability of organisational data.
- To protect IT resources from unauthorised access, misuse, or malicious activities.
- To establish clear guidelines for the use of IT systems.
- To comply with relevant legal and regulatory requirements.

Acceptable Use

General Guidelines

Users must use IT resources responsibly and solely for authorised business purposes. Personal use of IT resources should be minimal and not interfere with or compromise council business or consume excessive bandwidth.

Prohibited Activities

The following activities are prohibited:

- Accessing, downloading, or distributing illegal or inappropriate content.
- Using IT resources for unauthorised commercial purposes or personal gain.
- Attempting to breach network security or bypass IT controls.
- Installing unapproved software or hardware.

Data Security

Protection of Sensitive Information

All users must ensure that sensitive information is handled with care, stored securely, and accessed only by authorised personnel and compliant with the requirements of the Data Protection Act.

Access Control

Access to IT systems and data must be controlled through strong authentication methods. Employees are required to keep their login credentials confidential and report any suspected breaches immediately. Councillors are required to ensure that access to council emails addressed to them is suitably protected.

Backup and Recovery

The council will maintain regular backups of critical data and implement recovery procedures in case of data loss or system failures.

Network Security

Firewall and Antivirus Protection

All devices connected to the organisation's network must have updated antivirus software and be protected by firewalls to prevent cyber threats.

Monitoring

The clerk / RFO is the council's data protection officer and reserves the right to monitor network activity to ensure compliance with this policy and to detect unauthorised or suspicious behaviour.

Passwords

Passwords should be protected and changed as needed. Records of all passwords should be kept in a shared access online locked folder maintained by the Clerk and shared with the Chair and Deputy Chair.

Software Management

Licensing

All software used within the organisation must be appropriately licensed. The use of pirated or unlicensed software is strictly prohibited.

Updates

Software must be regularly updated to address vulnerabilities and ensure optimal functionality.

Incident Reporting

All IT incidents, including security breaches, hardware failures, or malware infections, must be reported to the Clerk immediately. Users must cooperate fully with investigations.

Training and Awareness

The council will where possible provide opportunities for training sessions to educate users on best practices for IT security, acceptable use guidelines, and recognising cybersecurity threats.

Compliance and Enforcement

Data Protection

Users should observe and abide by the six data protection principles as set out in the UK GDPR and Data Protection Act 2018 in relation to the processing of any personal data:

Lawfulness, fairness, and transparency

Purpose limitation

Data minimisation

Accuracy

Storage limitation

Integrity and confidentiality

Policy Violations

Violations of this policy will represent a breach of employment terms for employees and for councillors a breach of the code of conduct.

Audits

Regular audits will be conducted to ensure compliance with this policy and identify potential vulnerabilities.

Review and Updates

This policy will be reviewed annually or as needed to address advances in technology, changes in legal requirements, and evolving organisational needs.

Conclusion

By adhering to this IT policy, all users contribute to the security, efficiency, and integrity of the council's IT systems. This document aims to foster a culture of accountability and vigilance in the handling of digital resources.