IT Policy

Purpose: To establish clear parameters for how councillors, staff and other authorised individuals' access and handle council provided information technology and equipment in the course of their role.

Adopted: 12th March 2026 Minute Reference: 011 (a)

Review: March 2028

Introduction

Amberley Parish Council recognises the importance of effective and secure information technology (IT) in supporting its business and operations, this policy outlines the guidance and responsibilities for appropriate use by all users. This policy establishes the standard, responsibilities and security requirements for the use of information technology, email and digital communication systems provided or authorised by the council, ensuring compliance with GDPR, the data protection act 2018, the Freedom of Information Act 2000 and recognised best practice.

Scope

This policy applies to all individuals who use Amberley Parish Council's IT resources.
It covers:

- Council owned devices
- Approved personal devices
- Email and Communications systems
- Cloud services and storage
- Data handling and security
- Remote working

Roles and responsibilities

The Council

- Provides secure IT systems, devices and software
- Ensures compliance with statutory requirements
- Maintains appropriate security measures and access controls

The Clerk

- Acts as system administrator and primary contact
- Approves software installations and access permissions
- Leads on incident reporting, investigation and IICO notifications where required.
- Ensures data retention and archiving processed are followed.

Councillors, Staff and other Users

- Use council systems responsibly and securely
- Protect passwords, accounts and devices
- Report incidents immediately
- Use council email accounts for all council business

Acceptable use of IT resources and email

Amberley Parish Council's IT resources and email accounts are to be used for official council related tasks and activities. IT resources may be used for personal use as long as it is limited,

does not incur any costs to the council or adversely affects the performance of security of the IT systems. Personal use of the IT systems must not interfere with work responsibilities, incur cost to the Council, compromise security or violate any part of this policy. All users must adhere to ethical standards and respect intellectual property rights and copyright. Users must not access inappropriate, illegal or offensive material or install unapproved software or browser extensions.

Devise and software usage

Where possible the council will provide authorised devices, software and applications for work related tasks. All council owned devices remain the property of the Council and must be returned when the user leaves their role. Devices must not be altered, reset or disposed of without authorisation and must be kept updated with security patches and anti-virus software.

Only authorised software may be installed and unlicensed or pirated software is strictly prohibited.

Data Management and Security

All sensitive and confidential data should be stored and transmitted securely and using approved methods. Cloud storage improves reliability and security and only approved storages systems such as Microsoft 365 (SharePoint, OneDrive) are the preferred method of data management. Local storage on Council owned devices is permitted.

Email Communication

Members cannot use personal email accounts for Council business. Councillors will be issued with official email addresses which must be used for official communication only.

All users must be vigilant about phishing attempts, must not open suspicious attachments or links and use two-factor authentication where available.

Emails should be retained in accordance with the council's publication scheme.

The Council reserves the right to monitor email communications to ensure compliance with this policy and relevant legislation. Monitoring is conducted in line with UK GDOR Article 6(1)(f) – legitimate interest.

Password and account security

The council are responsible for maintaining the security of their data, accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security and two-factor authentication should be used when possible.

Mobile devices and remote work

Mobile devices provided by the council should be secured with passwords and/or biometric authentication. Public WiFi should be avoided unless using a secure VPN.

Reporting and security incidents

All suspected security breaches or incidents should be reported to the Clerk immediately for investigation and resolution including: lost or stolen devices, mis-sent emails, unauthorised access or data breaches.

Training and Awareness

Regular training and resources to educate users about IT security best practice, privacy concerns and technology updates will be provided.

Compliance and Consequences

Breach of this IT and Email policy may result in the suspension of IT privileges. Non-compliance with this policy may also trigger an investigation under the council's disciplinary policy, especially where data breaches are involved or a report to the Monitoring Officer for a potential breach of the council's adopted Code of Conduct.

Policy Review

This policy will be reviewed every two years or sooner is required by legislative or technological changes.