IT & Device Use Policy

Adopted March 2026

Purpose

This policy sets out minimum requirements for the use of information technology in the course of council business and to protect personal data in line with the Council's Data Protection Policy and the UK GDPR.

Scope

This policy applies to all Councillors, the Clerk, and any authorised persons who access or handle council data, whether using council equipment or personal devices.

Council Equipment

The Council provides limited IT equipment for council business. Additional equipment may be introduced as operational needs change.

Council equipment must be used for council business. Limited personal use is permitted provided it does not interfere with council duties, compromise security, or breach other Council policies.

Use of Personal Devices

Council business may involve accessing email or downloading documents on personal devices.

All council-related documents or data downloaded to personal devices must be deleted as soon as the task is completed.

Users must ensure devices are protected by a password or PIN, kept up to date with security updates, and do not store council data in personal cloud services.

Passwords and Authentication

Strong passwords or PINs must be used to access council systems. Multi-Factor Authentication (MFA) should be enabled wherever available.

Passwords must not be shared or written down insecurely.

Security and Data Protection

All personal data processed for council purposes must be handled in accordance with the Council's Data Protection Policy.

Devices used for council business must not be left unattended in public places and public Wi-Fi should be avoided unless secure connections are used.

Council data stored electronically must be backed up using secure methods appropriate to the systems in use. Where data is stored on personal devices, users must ensure that important council documents are saved to a secure council-controlled location where possible.

Use of Artificial Intelligence Tools

Publicly available artificial intelligence (AI) tools must not be used to process personal, confidential, or sensitive Council information unless specifically authorised.

Users must not input council documents, personal data, or non-public information into external AI systems.

Email

Council business should be conducted using official council email accounts wherever possible. Care must be taken to avoid the accidental disclosure of personal data.

Website and Online Services

Council online services and website content must be managed securely and in accordance with applicable legal requirements.

Personal data must not be published online unless there is a lawful basis to do so.

Social Media

Use of social media must comply with the Council's Social Media Policy. Councillors and staff must not represent personal views as those of the Council or disclose council information without authorisation.

Data Breaches

Any loss, theft, or suspected data breach involving devices used for council business must be reported immediately to the Clerk and handled in accordance with the Council's Data Protection Policy.

Misuse

Misuse of IT systems or failure to comply with this policy may result in withdrawal of IT access and, where appropriate, further action.

Review

This policy will be reviewed annually or when significant changes to council IT arrangements occur.