



Diss Town Council – Information Technology (IT) Policy

Introduction

Diss Town Council relies on information technology to support its day-to-day operations, communicate with residents and stakeholders, and enable councillors, employees and others to carry out their duties effectively. The Council recognises that the use of IT brings both benefits and risks. A clear policy framework helps reduce those risks and promotes responsible, secure and lawful use of technology.

This policy is based on guidance issued by the National Association of Local Councils (NALC) and has been adapted for use by Diss Town Council. It should be read alongside the Council's Standing Orders, Financial Regulations, Data Protection Policy and other related policies.

Purpose of the IT Policy

The purpose of this policy is to establish clear parameters for how IT systems and equipment provided by Diss Town Council may be used. In particular, this policy aims to:

- Set expectations for appropriate and acceptable use of IT systems.
 - Protect the confidentiality, integrity and availability of Council data.
 - Reduce the risk of data loss, cyberattack or misuse of systems.
 - Ensure compliance with the UK GDPR, the Data Protection Act 2018 and other relevant legislation.
 - Clarify the responsibilities of councillors, employees, contractors and other authorised users.
-

Scope of this Policy

This policy applies to all councillors, employees, contractors, volunteers and any other persons authorised to use Diss Town Council IT systems. It applies to:

- All Council-owned computers, mobile devices and associated equipment.
 - All Council systems, including email, internet access and cloud services.
 - Personal devices where these are authorised for use in connection with Council business.
-

Monitoring of IT Use

As the provider of IT systems, Diss Town Council reserves the right to monitor the use of its IT equipment and services where there is a legitimate business or legal reason to do so.

Any monitoring undertaken will be proportionate and carried out in accordance with data protection legislation. Monitoring may be used for purposes including system security, maintenance, investigation of suspected misuse, or compliance with legal obligations.

Users should be aware that they do not have an expectation of absolute privacy when using Council IT systems.

Use of Computer Equipment

General Principles

IT equipment is provided primarily for Council business. Limited personal use may be permitted, provided that it:

- Takes place outside normal working hours or during breaks.
- Does not interfere with Council duties.
- Does not incur cost to the Council.
- Does not breach this or any other Council policy.

Users are expected to:

- Lock computers and devices when leaving them unattended.
- Shut down equipment at the end of the working day where appropriate.
- Take reasonable care of all IT equipment.

Failure to do so may result in disciplinary or other appropriate action.

Equipment Management

All Council IT equipment is recorded and asset-tagged. Users must not:

- Modify, dismantle or attempt to repair equipment without authorisation
- Install software, including screensavers and wallpapers, unless approved by the Council or its IT provider.
- Use personal storage devices unless permission has been given by the IT provider.
- Transfer files to a third party without the express permission of the Clerk.

Loss or damage caused through negligence may lead to disciplinary action or recovery of costs.

Portable Equipment and Mobile Devices

Portable equipment includes laptops, tablets and smartphones. Users must ensure that portable equipment:

- Is kept secure at all times
- Is not left unattended in vehicles or public places.
- Uses appropriate security controls, such as encrypted storage and strong authentication.
- Is reported to the Town Clerk as soon as possible if lost or stolen.
- Complies with the Council's Mobile Device Management and security requirements as set out in this policy.

Photography, audio recording or video recording at Council premises or at non-public meetings is not permitted without prior authorisation, unless statutory rights apply.

Mobile Phone and Telephony Use (Including Assertion 10 Compliance)

Diss Town Council recognises that mobile phones and telephony systems are essential tools for conducting Council business. Their use must be secure, proportionate and compliant with data protection, cybersecurity and governance requirements, including those aligned with Assertion 10 standards.

Use of Council-Issued Mobile Phones

Council-issued mobile devices must be used primarily for official business purposes. Limited personal use is permitted provided that it:

- Does not interfere with Council duties.
- Does not incur significant cost to the Council.
- Complies with all aspects of this IT Policy.

Excessive personal use of Council-issued phones is not permitted and may result in withdrawal of access or disciplinary action.

Use of Personal Mobile Phones for Council Business

Where personal mobile phones are authorised for Council business, users must:

- Use Council-approved applications and systems for communication.
- Not store Council data locally on the device unless authorised.
- Ensure Council data is only accessed via secure, approved platforms.
- Comply with the same standards as Council-issued devices.

Mobile Device Security Requirements (Assertion 10 Compliance)

To ensure compliance with recognised security and governance standards:

- All mobile devices used for Council business (Council-issued or authorised personal devices) must be enrolled in a Council-approved Mobile Device Management (MDM) system where required.
- Devices must be protected by:
 - Strong passwords or biometric authentication.
 - Automatic locking after a short period of inactivity.
 - Up-to-date operating systems and security patches.

The Council (or its IT provider) must be able to:

- Enforce security policies remotely.
- Remove Council data where necessary, including remote wipe.
- Restrict access to non-compliant devices.
- Certain devices may also require approved antivirus or endpoint protection software, as specified by the Council's IT provider.

Data Protection and Confidentiality

Users must ensure that:

- Confidential or personal data is not accessed, discussed or displayed in public or insecure environments.
- Phone calls involving sensitive matters are conducted in private where possible.
- Text messages, call logs or voicemail containing Council business are handled in accordance with data protection requirements.

- Council data is retained only for as long as necessary and deleted securely when no longer required.

Monitoring and Logging

Use of Council telephony systems, including mobile devices, may be monitored where there is a legitimate business or legal reason. This may include:

- Review of call usage patterns.
- Audit of device compliance with security requirements.

Loss, Theft or Misuse

Any loss, theft or suspected compromise of a mobile device used for Council business must be reported immediately to the Town Clerk and/or IT provider. Prompt reporting enables appropriate action, including remote locking or wiping of data.

Compliance and Enforcement

Failure to comply with this section may result in:

- Withdrawal of access to Council systems.
- Disciplinary action.
- Potential legal consequences where data protection legislation is breached.

Use of Personal Devices

The Council recognises that, in some circumstances, personal devices may be used for Council business. Any such use must be authorised in advance. Where permission is given, users must:

- Use a Council email account for Council business.
- Ensure Council data is not stored in personal cloud services.
- Keep devices up to date with security patches and updates.
- Ensure that Council data can be securely removed or remotely wiped if required.

In the event of legal proceedings or investigations, the Council may need temporary access to devices used for Council business.

Personal devices must not be configured to automatically forward Council emails or store Council data outside Council-approved systems.

Health and Safety

The Council will provide suitable workstations for employees who use display screen equipment as part of their role and will offer eye tests in accordance with health and safety legislation.

Any concerns relating to workstation safety or IT equipment must be reported to the Health and Safety Officer.

Passwords and Authentication

Password management software is provided by the IT Provider to ensure that passwords are strong and held securely. Passwords must not be shared, written down or stored insecurely.

Where available, Multi-Factor Authentication (MFA) must be enabled to provide additional protection against unauthorised access.

The Council's IT provider is responsible for managing system-level and service account credentials.

Remote Working

Additional care must be taken when working away from Council premises, including when working from home or while travelling. Users should:

- Use secure networks and approved devices.
- Avoid saving passwords on shared or public computers.
- Ensure screens cannot be overlooked by others.
- Save Council data to Council systems as soon as possible.

Confidential information must not be left unattended at any time.

Email

Council email facilities are provided to support effective communication on Council business. Users must use email in a professional and responsible manner. Users must not:

- Send offensive, discriminatory or inappropriate content.
- Commit the Council financially unless authorised to do so.

- Use Council email accounts for personal commercial activity.

Email use may be monitored in accordance with this policy.

Council Email Accounts and Domains

All Council business must be conducted using email accounts provided by Diss Town Council and hosted on a Council-owned domain.

The use of personal or free external email services for Council business is not permitted.

Email accounts, mailboxes and access rights remain the property of Diss Town Council and must be made available to the Council on request.

Use of the Internet

Internet access is provided to support Council business. Limited personal use may be permitted outside working hours where this does not interfere with duties. Internet use may be monitored by the Council.

The following activities are prohibited:

- Accessing illegal or inappropriate websites.
 - Downloading copyright material unlawfully.
 - Online gambling or illegal activities.
-

Use of Social Media

Social media includes social networking sites, blogs, forums and other online platforms. Users must ensure that their use of social media does not bring Diss Town Council into disrepute.

Councillors and employees must not present themselves as speaking on behalf of the Council unless authorised and must comply with the Members' Code of Conduct, the Nolan Principles and other relevant Council policies.

Website, Accessibility and Transparency

Last Reviewed: April 2026
Next Review: April 2029 (or sooner if legislation or guidance changes)

Diss Town Council recognises its obligations under the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018, the Freedom of Information Act 2000 and the Transparency Code for Smaller Authorities.

Council information published online will be managed in accordance with the Council's Website Accessibility Statement, Publication Scheme and Data Protection Policy.

Misuse of IT Systems

Misuse of IT systems or equipment is not in line with the Council's standards of conduct and will be taken seriously. Any breach of this policy may result in disciplinary action or other appropriate action in the case of councillors or contractors.

Review of the Policy

This policy will be reviewed by the Council at least every three years, or sooner where required by changes in legislation, technology or Council operations.

Approved by: Diss Town Council

Minute Reference: _____

Date Approved: _____