Ulverston Town Council

IT Policy

1. Introduction

Ulverston Town Council recognises the importance of effective, secure use of information technology (IT) and email in supporting its business, operations, and communications.

This policy sets out the expectations and responsibilities for the use of IT resources and email in connection with council business. It supports compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Freedom of Information Act 2000, the Environmental Information Regulations 2004, and other relevant legislation, and supports Assertion 10 of the Annual Governance & Accountability Return (AGAR).

2. Scope

This policy applies to all councillors, employees, contractors, volunteers, and other authorised users who access or use Ulverston Town Council's IT systems, data, or email for council business, whether using council-owned or personal devices and regardless of location.

3. Acceptable Use of IT Resources and Email

Ulverston Town Council's IT resources and email accounts are provided for official council business only. Limited personal use of Town Council equipment is permitted if it does not interfere with council work, incur additional cost, or breach any policy (such as staff accessing the internet on their lunch break).

Users must:

● Act professionally and respectfully

● Comply with copyright and intellectual property laws

● Avoid accessing, creating, or transmitting offensive, inappropriate, discriminatory, or illegal material

● Not use council systems for political campaigning, personal business, harassment, or activities that could bring the Council into disrepute.

Council email addresses must be on a council-controlled domain and used for official council business. All Ulverston Town Council emails are on the .org domain.

Personal email accounts must not be used for council matters under any circumstances.

Informal messaging apps (e.g., WhatsApp, SMS) may be used for routine coordination but must not be used to discuss or make decisions on council business or to store/share documents containing personal or confidential information.

4. Device and Software Usage

Where possible, authorised devices, software, and applications will be provided by Ulverston Town Council for work-related tasks.

● Unauthorised installation of software on council devices is prohibited

● All devices must use approved security controls including antivirus protection, automatic updates and encryption where applicable

● Security controls must not be disabled or bypassed

5. Use of Personal Devices

Councillors and authorised staff may use personal devices to access council email or information where this is necessary and appropriate. To protect council data and comply with data protection legislation, users must:

● Secure devices with a PIN, passcode, or biometric lock

● Keep devices updated with the latest security patches and operating system updates

● Ensure council information is not accessible to family members or other third parties

● Use only council-approved apps and storage

● Avoid storing council documents permanently on personal devices

● Not back up council data to personal cloud services

● Report lost or stolen devices immediately to the Town Clerk so access can be revoked if necessary

● Allow remote removal of council data if access ends or the device is compromised

● Ensure devices used for council business are not shared with others while logged in to council systems

6. Data Management and Security

All sensitive and confidential Ulverston Town Council data must be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

Personal data must be processed lawfully, fairly, and transparently in accordance with the Council's Data Protection and Privacy Policy. Users are responsible for protecting personal data from unauthorised access, disclosure, loss, or destruction.

7. Network and Internet Usage

Ulverston Town Council's network and internet connections should be used responsibly and efficiently for official purposes.

● Downloading or sharing copyrighted material without authorisation is prohibited

● Access to websites or services that pose a security risk may be restricted

● Users must not attempt to bypass security or filtering controls

8. Email Communication

Email accounts provided by Ulverston Town Council are for official communication only.

● Emails should be professional and respectful in tone

● Users should be cautious with attachments and links to avoid phishing and malware

● Council business must not be conducted using personal email accounts

● Emails may be subject to Freedom of Information or Environmental Information requests

9. Password and Account Security

Users are responsible for maintaining the security of their accounts and passwords.

● Passwords should be strong, unique, and not shared

● Regular password changes are encouraged

● Multi-factor authentication (MFA) must be used where feasible

● Passwords and account access must meet recognised cybersecurity standards

10. Remote Work

Users working remotely must follow the same security practices as if in the office.

Where personal devices are authorised for council use, the Council may enforce security controls and remove council data if necessary.

11. Monitoring

Ulverston Town Council may monitor IT and email usage to:

● Ensure compliance with this policy

● Protect council systems

● Investigate suspected misconduct

● Meet legal or regulatory obligations

Monitoring will be proportionate, lawful, and in line with data protection legislation. Personal communications will be respected wherever possible.

12. Retention and Archiving

Emails must be retained and archived in accordance with legal and regulatory requirements.

● Regularly review and delete unnecessary emails

● Emails and electronic records must be managed in accordance with the Council's Document Retention Policy

● Records must not be destroyed to prevent access for statutory requests (FOI/SAR)

● Email archiving solutions should ensure council-wide access independent of individual devices/accounts

13. Reporting Security Incidents

All suspected security breaches or incidents must be reported immediately to the Clerk for investigation and resolution.

Any personal data breach must be reported immediately to the Town Clerk to enable assessment and, where required, notification to the Information Commissioner's Office within statutory timescales.

14. Training and Awareness

Ulverston Town Council will provide training and appropriate resources to educate users about IT security best practices, privacy concerns, and technology updates.

Users are responsible for familiarising themselves with this policy and related policies, including the Data Protection and Privacy Policy and the Document Retention Policy.

15. Compliance and Consequences

Breach of this IT Policy may result in:

- Suspension of IT privileges
- Disciplinary action for employees
- Action under the Councillors' Code of Conduct
- Termination of access for contractors
- Legal action where appropriate

16. Policy Review

This policy will be reviewed by the Town Clerk and Council annually to ensure its relevance and effectiveness. Updates may be made at any time to address emerging technology trends and security measures.

17. Contacts

For IT-related enquiries or assistance, users can contact the Town Clerk.

Ulverston Town Council is the Data Controller for the purposes of data protection legislation.

Acknowledgement

All staff and councillors are responsible for the safety and security of Ulverston Town Council's IT and email systems. By adhering to this policy, the Council aims to create a secure and efficient IT environment which supports its operations.

Approved by Ulverston Town Council: May 2026

Minute no: D018

Due for review: May 2027