Urpeth Parish Council

IT, Digital and Information Security Policy

1. Purpose

This IT, Digital and Information Security Policy sets out how Urpeth Parish Council manages its information technology systems, electronic records and digital communications. The policy ensures that information is handled securely, lawfully and efficiently, while remaining proportionate to the size and capacity of a small Parish Council with three employees and eleven councillors. The policy is intended to support good governance, compliance with relevant legislation and guidance, and the Council's obligations under the Annual Governance and Accountability Return, in particular Assertion 10 relating to information governance.

2. Scope

This policy applies to all councillors, employees and any contractors or volunteers who access council information or IT systems. It covers the use of council-owned and approved personal devices, including desktop computers, laptops, tablets and mobile phones, as well as the use of email systems, cloud storage, websites, digital records and electronic communications. The policy applies equally to work undertaken in council offices, at home, or in any other location where council business is conducted.

3. Legal and Regulatory Framework

The Council recognises its responsibilities under the UK General Data Protection Regulation and the Data Protection Act 2018 to ensure that personal data is processed lawfully, fairly and securely. The policy also supports compliance with the Freedom of Information Act 2000, the Local Government Transparency Code, the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018, and guidance issued by the Information Commissioner's Office and the National Association of Local Councils. The Council is committed to maintaining appropriate information security arrangements in accordance with AGAR Assertion 10.

4. Governance and Responsibilities

The Council is collectively responsible for approving this policy and ensuring that appropriate and proportionate measures are in place to manage IT and information security risks. The Proper Officer has responsibility for overseeing the day-to-day

operation of this policy and ensuring that IT arrangements remain suitable for the Council's needs. The Responsible Financial Officer is responsible for ensuring that financial systems and data are appropriately secured. All councillors and employees have a personal responsibility to comply with this policy, to act prudently when using IT systems, and to report any concerns, breaches or suspected incidents without delay.

5. IT Systems and Equipment

Council-owned IT equipment is provided solely for the conduct of council business and must be used responsibly. Such equipment must be protected against unauthorised access through the use of passwords, PINs or biometric controls and must be kept up to date with operating system updates and security patches where reasonably practicable. Council equipment must not be shared with unauthorised individuals and must be returned when no longer required or when a councillor or employee leaves office.

Where the use of personal devices is necessary to support council business, this is permitted on a limited and proportionate basis. Personal devices used for council purposes must be adequately secured and council information must not be retained on such devices longer than necessary. The Council accepts no responsibility for the maintenance, security or loss of personal devices.

6. Access Control and Password Security

Access to council IT systems, email accounts and digital records is limited to those who require it to carry out their role. Strong passwords must be used and must not be shared with others. Users are required to take reasonable steps to protect login credentials and to ensure that devices are locked when not in use. Access rights must be reviewed periodically and must be removed promptly when a councillor or employee leaves office or no longer requires access.

7. Email, Internet and Digital Communications

Council business should be conducted using council-provided email accounts wherever practicable in order to maintain proper records and ensure transparency. Personal email accounts should not be used for sensitive or confidential council business. Users must exercise caution when opening email attachments or following links to reduce the risk of cyber threats. Councillors and employees are reminded that council communications may be subject to disclosure under the Freedom of Information Act.

8. Mobile Phone Use

Where council-issued mobile phones are provided, they are to be used for council business only and must be protected by appropriate security measures such as PINs or biometric locks. In cases where personal mobile phones are used for council business, users must ensure that council data is kept secure and removed when no longer required. Informal messaging applications should not be used for formal decision-making or the exchange of sensitive information, and councillors should ensure that council business is conducted in a manner that remains transparent and properly recorded.

9. Data Protection and Information Security

The Council will only collect, retain and process information that is necessary for the performance of its statutory and administrative functions. Personal data must be handled in accordance with the Council's Data Protection Policy and retained only for as long as is necessary. Reasonable measures will be taken to protect information from loss, unauthorised access or disclosure, whether held electronically or in paper form. Secure disposal methods must be used when information is no longer required.

10. Data Breaches and Cyber Incidents

Any actual or suspected data breach, cyber incident, loss of equipment or unauthorised access to information must be reported immediately to the Proper Officer. Incidents will be logged, investigated and assessed to determine whether reporting to the Information Commissioner's Office or affected individuals is required. The Council will take appropriate remedial action to reduce the risk of recurrence.

11. Backup and Business Continuity

The Council will take proportionate steps to ensure that important digital records are backed up regularly and can be recovered in the event of system failure, loss or cyber incident. Reliance on a single device or individual for access to essential information will be avoided wherever possible to support business continuity.

12. Website Management and Accessibility

The Council is committed to ensuring that its website is accessible and compliant with the Web Content Accessibility Guidelines (WCAG) 2.2 at AA level, insofar as is reasonably practicable. An accessibility statement will be published and reviewed regularly. Documents published on the website will be provided in accessible formats

where possible, and the Council will make reasonable adjustments to address accessibility barriers when identified.

13. Transparency and Publication of Information

Statutory information will be published in accordance with transparency requirements. Care will be taken to ensure that personal data and confidential information are not disclosed inadvertently. Information will be reviewed and redacted where necessary prior to publication.

14. Training and Awareness

The Council recognises the importance of ensuring that councillors and employees have an appropriate understanding of IT security and data protection. New councillors and staff will receive basic guidance, and periodic reminders or updates will be provided to reflect emerging risks or changes in practice.

15. Monitoring and Review

Compliance with this policy may be monitored periodically, and any non-compliance will be addressed appropriately. This policy will be reviewed at least every two years, or sooner if there are significant changes in legislation, technology or council operations.

Adopted: 19 May 2026

To be reviewed at least every two years or when change in legislation or council operations.