Dersingham Parish Council
Information Technology (IT) Policy

1. Purpose

This policy defines how Dersingham Parish Council manages its use of information technology, in line with the Transparency Code for Smaller Authorities (2015) and the 2025 edition of the Practitioners' Guide. It ensures the council's digital operations are transparent, secure, and compliant with data protection laws.

2. Scope

This policy applies to all councillors, employees, volunteers, and contractors who access or manage the council's IT resources, including but not limited to:

- Desktop and laptop computers, tablets, and smartphones
- Email and cloud-based systems
- Council website, social media, and digital publication tools
- Video conferencing and messaging platforms
- Personal devices used under Bring Your Own Device (BYOD) provisions of this policy

3. Governance and Oversight

The Business Manager is the designated Data Protection Officer (DPO). IT systems support and administration is mainly provided by cloud service suppliers or contractors with some local administration of email and office systems being provided by a designated councillor and/or officer. The Finance & Administration Committee oversees implementation, security, and compliance of existing and new IT systems.

4. Data Protection & Security

All processing of personal data shall comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

4.1 Privacy Policy

All data collection, processing, and subject rights are governed by the council's Privacy Policy, available on the council public website. All users must familiarise themselves with it.

4.2 Access and Storage

Data is stored securely with access granted only to authorised personnel based on necessity. Appropriate backup procedures are in place to secure all critical systems and data and test restores must be carried out periodically.

4.3 Retention

Personal data will be retained in accordance with the council's Data Retention Schedule and securely deleted when no longer needed.

4.4 Security Controls

All Parish Council systems shall be secured with user specific strong passwords and multi-factor authentication where appropriate.

- All users of Parish Council systems are responsible for maintaining the security of their accounts and passwords. Regular password changes are encouraged to enhance security.
- User ID's and passwords must not be shared with others.
- The use of biometric authentication and/or passkeys is encouraged where available.
- All devices used to access Parish Council systems should be configured to receive regular security and anti-malware software updates.
- Information stored in council systems other than the public website is intended for use by authorised users only and must not be shared with others without the formal agreement of the Business Manager.
- When working remotely, users should follow the same security practices as if they were in a Parish Council Office.
- When attending meetings remotely, users must ensure they comply with the Parish Councils remote meetings protocol.
- No software should be installed on council owned devices by users without the specific formal authorisation from the Business Manager.

5. Use of Personal Devices (BYOD)

In this section, the term "authorised person" refers to an individual councillor, staff member, or guest registered user who has been granted access to use, or support, one or more of the councils IT systems.

Authorised persons may use their personal devices, including personal computers, and mobile devices, to access Parish Council services including email. These services may be securely accessed using a web browser from any device connected to the internet.

5.1 Authorised Use

The authorised person may use their personal devices to access council systems for council business subject to compliance with this policy.

5.2 Security Requirements

The device used must be configured for the exclusive use of the authorised person OR employ appropriate security measures to prevent the councils systems or data, from being accessed by anyone other than the authorised person.

Personal computers, laptops and mobile devices must be secured by user ID and password or other means appropriate to the device to prevent access by unauthorised persons. The use of modern authentication including biometric authentication and multi-factor authentication is encouraged.

Devices must be protected by strong passwords, biometric authentication encryption (where possible), and up-to-date antivirus software. Access to council data on personal devices will be controlled and subject to regular review.

Devices used by persons other than an authorised person may only be used to access council systems using a web browser. The following conditions must also be complied with:

- Usernames and passwords for the council systems must not be cached on the local device and passwords must be securely maintained by the authorised person. Biometric authentication and PIN codes may be used provided the device is designed for multiple user use.
- Care is taken to securely log out of the councils system at the end of each work session and when leaving the device unattended.
- No council documents or emails are to be stored locally on the device or be copied to any storage location accessible by anyone other than the authorised person.

5.3 Data Separation

Council data stored on authorised persons own device must be kept separate from personal data using dedicated apps or storage separate areas and must not be accessible by persons other than the authorised person.

6. Acceptable use of IT systems

The IT systems provided by the Parish Council are to be used for council related activities and business only. Limited personal use is permitted provided it does not interfere with work responsibilities or violate any part of this policy.

Non-council related data must not be stored in any parish council system.

Users must not install software on or reconfigure any Parish Council owned computer or mobile device without the specific authorisation of the Business Manager.

All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing or distributing inappropriate or offensive content.

7. Use of Email for Council Business

All councillors and staff are provided with Parish Council email accounts to be used for all official email communication.

- **The use of personal email accounts for council business is strictly prohibited**. All council correspondence must be conducted through official council-provided mail addresses.
- Emails sent to council-owned mail addresses must not be auto-forwarded to personal email addresses.
- Councillors and staff must not permit anyone else to access or view their council mailboxes or individual mail items. Special care must be taken when viewing email in a public place.
- All users of the council mail system must remain alert to the risks from phishing emails and malware. Verify the source before opening attachments or clicking on links to unfamiliar systems or websites.
- Emails should be professional in language and respectful in tone.
- Confidential or sensitive information must not be sent via email unless it is encrypted.
- Dersingham Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

- Any breaches of this policy or relevant laws will be investigated, and appropriate measures taken in line with the council's disciplinary or governance procedures.
- Council emails should be retained in compliance with the councils document retention policy, GDPR and Freedom of Information Act requirements.

8. IT Infrastructure & Support

An Asset register shall be maintained for all council-owned hardware and software.

All council owned devices are to be configured to receive security and other critical software updates as soon as they are available. Users of these devices are responsible for reporting any error or warning messages that they cannot resolve to the Business Manager without delay. The Business Manager is responsible for ensuring any reported issues are resolved as soon as is practically possible commensurate with the severity of the issue.

The Business Manager shall ensure that all Council owned devices are checked at least annually for compliance with this policy.

Users will be given appropriate training on IT systems, cybersecurity, data handling, and transparency responsibilities.

9. Public Website

Dersingham Parish Council is committed to making its public website accessible in accordance with the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018.

An accessibility statement must be published on the website to clearly state the level of web accessibility to which the website aims to conform.

10. Monitoring and Review

This policy will be reviewed annually, or sooner if legislation changes.

The Business Manager shall be responsible for ensuring that periodic internal audits check for compliance with security and transparency requirements.

11. Data Breach Process and Protocols

The Parish Council is committed to responding promptly and effectively to any data breaches to minimise risk and comply with UK GDPR requirements.

11.1 Definition of a Data Breach

A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:

- Loss or theft of devices containing personal data
- Unauthorised access to council email accounts or files
- Sending personal data to the wrong recipient
- Malware or ransomware attacks compromising council systems

11.2 Reporting a Breach

Immediate Notification: Any councillor, employee, or contractor who becomes aware of a data breach must report it immediately to the Business Manager (Data Protection Officer).

Initial Response: The Business Manager will assess the severity and scope of the breach and determine if mitigation steps are required (e.g., changing passwords, disabling access, enabling 2FA).

11.3 Investigation

A full investigation will be conducted by the Business Manager or designated officer within 72 hours of the breach being discovered. The breach will be logged, including:

- Date and time of breach
- Type and volume of data affected
- Cause and extent of the breach
- Actions taken to address the breach

11.4 Notification Requirements

If the breach is likely to result in a risk to the rights and freedoms of individuals, the council must notify the Information Commissioner's Office (ICO) within 72 hours.

If the breach poses a high risk to the individuals affected, those individuals must also be informed without undue delay, outlining:

- The nature of the breach
- Likely consequences
- Measures taken to mitigate the risk
- Contact information for further support

11.5 Remediation and Review

The Business Manager and the Finance & Administration Committee will ensure lessons are learned and policies, procedures, or training are updated as necessary.

Technical fixes or security upgrades will be prioritised to prevent recurrence.

Breach logs will be reviewed to identify systemic issues.

12. Approval and Adoption

This policy was adopted by Dersingham Parish Council on 24th November 2025 and will be reviewed annually or following a significant incident or legislative change.