COVENEY PARISH COUNCIL

IT POLICY
2025

Parish Council Information Technology (IT) Policy of Coveney Parish Council

Version 1.1 – Adopted October 2025[1]

1. Purpose

This policy outlines how Coveney Parish Council manages its use of digital and information technologies. It aligns with the Transparency Code for Smaller Authorities (2015) and the 2025 edition of the Practitioners' Guide, ensuring secure, transparent and legally compliant digital operations.

2. Who it applies to

This policy covers all individuals involved with the Council's IT systems including:

- Councillors
- Staff and volunteers
- Contractors and third-party providers

The following systems and tools fall under this policy:

- Computers, tablets, and smartphones
- Council managed email and cloud-based systems
- Official website, social media platforms
- Video conferencing tools and messaging apps
- Any personal devices used under Bring Your Own Device (BYOD) policy.

3. Management and Oversight

IT Leadership: The Clerk acts as both the Data Protection Officer (DPO) and IT Systems Administrator.

4. Data Protection & Security

The Council adheres strictly to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Key Security measures:[2] (for Council owned devices)

- Use of strong passwords and multi-factor authentication (MFA)
- Installation of antivirus software and system updates
- Routine backups to secure storage

Data Access: Restricted to authorised personnel only and reviewed regularly.

Data Retention: Personal Data will be retained only for as long as necessary for Council business and deleted.

Privacy Policy: All users must follow the Council's privacy policy, available on the official website.

5. Use of Personal Devices (BYOD)

Authorisation Required: Only authorised personnel may use personal devices for Council tasks.

Security Requirements: Devices must be appropriately secured, for example with strong passwords or antivirus software. Council data must be clearly identifiable in case a subject access request is made.

6. Council Email Policy

All council email communication[3] must take place through Council provided email accounts. Email forwarding is not permitted from Council email accounts to Councillor's personal email accounts.

Violations will be addressed in accordance with the Council procedures.

Emails will be retained in line with the GDPR and Freedom of Information (FOI) standards.

7. IT Infrastructure & Support

Asset Register: Maintained for all Council-owned hardware and software.
Maintenance: All Council devices[4] must be regularly updated and checked for compliance with this policy.
Training: Councillors and staff will be given basic online training on IT systems, cybersecurity, data handling, and transparency responsibilities.

8. Monitoring and Review

Annual Review: This policy will be reviewed annually, or sooner if legislation or requirement changes.
Audits: Periodic internal audits will check for compliance with security and transparency requirements.

9. 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.

10. 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

10.1 Reporting a Breach

Immediate Notification: Any Councillor, employee, or contractor who becomes aware of a data breach must report it immediately to the Clerk (Data Protection Officer).
Initial Response: The Clerk will assess the severity and scope of the breach and determine if mitigation steps are required (e.g., changing passwords, disabling access, enabling 2FA).

10.2 Investigation

A full investigation will be conducted by the Clerk 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

10.3 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

10.4 Remediation and Review

▪ The Clerk 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 periodically to identify systemic issues.

11. Approval and Adoption

This policy was adopted by Coveney Parish Council on 20th October 2025 and will be reviewed annually or following a significant incident or legislative change.

Signed:

Chair of the Parish Council

Signed:

Clerk to the Parish Council

DATE: