Ryhall Parish Council
Data Security Policy

Policy Adopted: 07/09/2026
Reviewed: In accordance with the Document Review Schedule

1. Introduction
Ryhall Parish Council is committed to protecting all information it holds, whether digital or paper-based. This Data Security Policy sets out the principles, responsibilities, and procedures required to safeguard council data, ensuring compliance with GDPR, the Data Protection Act 2018, and the council's IT Policy. This policy works in conjunction with the **Ryhall Parish Council IT Policy**, which outlines the technical and operational controls for secure IT and email usage.

2. Scope
This policy applies to all councillors, employees, volunteers, contractors, and any individuals who handle Ryhall Parish Council data in any form, including:

- Digital files
- Emails
- Paper records
- Photographs, audio, and video
- Backups and archived materials

3. Governance and Oversight
The Clerk is the designated **Data Protection Officer (DPO)**, as stated in the IT Policy. The DPO oversees compliance, training, incident reporting, and data-handling standards.
Training will be provided by Ryhall Parish Council, Rutland County Council, and LRALC.

4. Data Classification
Council data will be categorised as:

- **Public Information** – intended for publication or public access
- **Internal Administrative Data** – routine working documents
- **Confidential Data** – personal data, financial information, legal matters
- **Highly Sensitive Data** – safeguarding, disciplinary, or security-related information

Handling requirements increase with sensitivity.

5. Secure Storage and Transmission of Data
All sensitive and confidential data must be stored and transmitted securely using the council's approved systems, including:

- **Zoho Mail and Zoho platform** for secure email and data storage (encrypted at rest and in transit).
- **Microsoft 365** and **local hard-drive backups** for Clerk documents.
- **Core Creatives** for website management and backup processes.

Paper records must be stored in cabinets within the clerks office secured home-working environment.

6. Access Control
Access to council data will be granted on a "least privilege" basis:

- Councillors may access information relevant to their role.
- Staff may access operational data required for their duties.
- Sensitive data is restricted to authorised personnel only.
- Personal accounts must **never** be used for council business, as stated in the IT Policy.

7. Device and Software Security

Only authorised devices and software may be used for council work. The IT Policy states:
"Unauthorised installation of software on authorised devices… is strictly prohibited due to security concerns."

All devices must have:

- Up-to-date antivirus protection
- Regular security updates
- Strong passwords and 2FA (Zoho authenticator recommended)
- Secure Wi-Fi or VPN when working remotely
-

8. Data Backup and Recovery

Backups must be performed regularly to prevent data loss.
Current arrangements include:

- **Zoho Mail** backup and recovery (deleted emails retained for 30 days).
- **Website backups** via hosting provider and Core Creatives tools.
- **Clerk document backups** on hard drive and Microsoft 365.

The DPO will ensure backup systems remain effective and tested.

9. Data Sharing and Transfer

Data must only be shared:

- With authorised individuals
- Through secure channels (Zoho Mail, encrypted attachments, secure cloud links)
- When necessary for council operations
- In compliance with GDPR principles

Personal data must never be transferred to personal email accounts or devices.

10. Physical Security of Paper Records

Paper documents must be:

- Stored in locked cabinets
- Transported securely
- Shredded using cross-cut shredders when no longer required
- Never left unattended in public or shared spaces

11. Email Security

Email communication must follow the IT Policy, including:

- Professional and respectful tone
- Caution with attachments and links
- Verification of sender identity
- Use of Zoho's encrypted email system
- Avoiding personal accounts for council business

12. Data Retention and Archiving

Retention periods must follow legal requirements and align with Zoho's retention features:

- Deleted emails retained 5–180 days, then an additional 30 days.
- Terminated accounts retained for 3 months; inactive unpaid accounts for 120 days.
- Paper records retained according to statutory schedules (e.g., financial records, minutes, contracts).
- Regular review of stored data to remove unnecessary items.

13. Reporting Data Security Incidents
All suspected breaches must be reported immediately to: The Clerk/DPO for data protection concerns
This mirrors the IT Policy requirement:
"All suspected security breaches or incidents should be reported immediately…" Incidents will be logged, investigated, and reported in accordance with GDPR.

14. Training and Awareness
Regular training will be provided on:

- Data protection responsibilities
- Secure handling of personal data
- Email and cyber-security
- Updates to IT systems and procedures

This aligns with the IT Policy's commitment to ongoing training.

15. Compliance and Consequences
Failure to comply with this policy may result in:

- Suspension of IT access
- Formal warnings
- Referral to external authorities where required

This mirrors the IT Policy's compliance section.

16. Policy Review
This policy will be reviewed annually or sooner if required due to:

- Legislative changes
- New technologies
- Updated security practices
-

17. Contacts
For data security enquiries, contact: **Clerk / Data Protection Officer** Email: clerk@ryhallparishcouncil.gov.uk