OVING PARISH COUNCIL
IT & Data Management Policy

1. Purpose

This policy sets out how Oving Parish Council manages information technology, electronic communications and data in a secure, lawful and auditable manner.

It consolidates previous IT and data governance provisions into a single, authoritative policy.

The policy supports compliance with:

- UK GDPR and the Data Protection Act 2018
- Freedom of Information Act 2000
- Local Government transparency requirements
- Audit requirements, including governance and accountability standards

2. Scope

This policy applies to:

- Councillors
- Employees
- Contractors, consultants and locum staff
- Any person accessing Council IT systems or handling Council data

It covers all Council-owned or Council-controlled:

- Computers, laptops, tablets and mobile devices
- Email accounts and cloud-based systems
- Websites, social media and digital communications
- Data stored electronically or backed up by third parties

3. Roles and Responsibilities

Council: Oving Parish Council is responsible for approving this policy and ensuring appropriate systems and controls are in place.

Clerk / Responsible Officer responsibilities include:

- Overseeing day-to-day compliance with this policy
- Ensuring systems are used appropriately
- Ensuring data is retained and disposed of in line with the Retention and Disposal Policy
- Reporting any data breaches or IT incidents

All users must:

- Use Council systems responsibly and lawfully
- Protect passwords and access credentials
- Report any suspected data breach, loss or misuse immediately

4. Acceptable Use of IT Systems

Council IT systems must be used primarily for Council business.

Limited personal use may be permitted provided that it:

- Does not interfere with Council business
- Does not incur additional cost
- Does not breach confidentiality or security

IT systems must not be used for:

- Unlawful activity
- Offensive, discriminatory or inappropriate material
- Personal commercial activity

5. Email Use and Management

Councillors and officers should use Council-provided email accounts for Council business wherever possible.

Where personal email accounts are used for Council business, information remains subject to FOI and data protection legislation.

Emails are records and must be managed in accordance with the Council's Retention and Disposal Policy.

Routine or transitory emails should not be retained longer than necessary.

Emails evidencing decisions, approvals or financial transactions must be retained in line with audit requirements.

6. Data Protection and Information Security

All personal data must be processed lawfully, fairly and transparently, kept secure, limited to what is necessary for Council purposes, and retained only for as long as required.

The Council will:

- Use password protection and access controls
- Ensure antivirus and system updates are applied
- Restrict access to sensitive data to authorised users only

Users must not:

- Share passwords

- Store Council data on unapproved devices or platforms
- Bypass security controls

7. Third-Party Systems and Cloud Storage

Data stored on third-party systems (including cloud providers) is considered data held on behalf of Oving Parish Council.

Contracts with third-party providers must include appropriate data protection and security provisions.

The Council will ensure that retention and deletion arrangements can be applied to third-party systems.

8. Website and Digital Communications

The Council website will be used to publish statutory information, provide transparency and access to Council business, and communicate with residents.

The Clerk is responsible for ensuring information published is accurate, up to date and compliant.

Social media accounts are Council assets and must be used in accordance with agreed protocols. No personal data should be shared unless lawful and necessary.

9. Records Management and Retention

Signed Council and Committee minutes, AGAR returns, annual accounts and audit reports are retained permanently.

Routine financial records are retained for a minimum of six years plus the current financial year.

This policy operates alongside the Retention and Disposal Policy.

Deletion of data must be authorised and documented where appropriate.

10. Data Breaches and Incidents

Any actual or suspected data breach, loss of data, or unauthorised access must be reported immediately to the Clerk.

The Clerk will assess the incident, take remedial action, and report to the ICO where required.

11. Monitoring and Review

This policy will be reviewed at least every two years, or sooner if legislation or guidance changes.

Training will be provided where necessary to support compliance.

12. Adoption and Status

This policy replaces any previous IT or data management policies adopted by Oving Parish Council.

This policy should be read in conjunction with the Data Protection Policy and Retention and Disposal Policy.

Adopted by Oving Parish Council: 19 March 2026

Review date: 2027