PORLOCK PARISH COUNCIL
POLICY: GDPR & DATA PROTECTION
DATA & IT COMPLIANCE PACK

Purpose
Porlock Parish Council is committed to secure, responsible, and compliant handling of information technology and personal data. This combined policy pack aligns the Council's IT & Digital Policy, and GDPR/Data Protection obligations including Retention & disposal, fully incorporating 2025 Practitioners' Guide Assertion 10 – Digital & Data Compliance.

1. Scope

Applies to all councillors, employees, volunteers, contractors, and third-party providers accessing Council IT systems, email, data, or digital platforms, in any format (electronic, paper, cloud).

2. Roles & Responsibilities

Role	Responsibility
Clerk / RFO	Data Protection Officer; ensures overall compliance, audits, manages incidents, liaises with ICO.
Councillors, Staff & Volunteers	Follow policy, report incidents, ensure secure handling of personal data, attend annual GDPR and IT security training.
Third-Party Contractors	Process data only as instructed; maintain security standards; sign data protection agreements.

3. Council-Owned Domains & Email Management

Porlock Parish Council operates one secure domain:

- **porlockparishcouncil.gov.uk** – officers, staff and councillors

All official communications must use these domains. Personal emails are prohibited for council business. Passwords must be strong, unique, and MFA-enabled. Accounts are issued, monitored, and revoked under the Clerk's authority.

4. Data Inventory

The council maintains a comprehensive Data Inventory covering all categories of digital and paper records, including emails, cloud storage, and physical documents. For guidance on retention periods, disposal methods, and legal compliance, see the Retention & Disposal Policy (2026).

5. Privacy Notices

1. Residents / Public
   Purpose: Inform how data is collected, used, and stored.
   Controller: Porlock Parish Council
   Data: Name, contact, enquiry info
   Purpose: Respond to enquiries, services, updates, legal obligations
   Lawful basis: Legal obligation, legitimate interests, consent
   Sharing: Only approved providers, legal obligations
   Retention: See Retention & Disposal Policy (2026)
   Rights: Access, rectify, restrict, deletion
   Contact: clerk@porlockparishcouncil.gov.uk

2. Staff/Employees
   Controller: Porlock Parish Council

Data: Name, address, NI, bank, employment records
Purpose: HR, payroll, benefits, legal compliance
Lawful basis: Employment contract, legal obligations
Sharing: Payroll, HMRC, pensions
Retention: See Retention & Disposal Policy (2026)
Rights: Access, rectify, restrict, deletion
Contact: clerk@prolockparishcouncil.gov.uk

3. Councillors
Controller: Porlock Parish Council
Data: Name, contact, committee membership
Purpose: Council communications, meeting management
Lawful basis: Legal obligation, legitimate interests
Sharing: Published for transparency as required
Retention: See Retention & Disposal Policy (2026)
Rights: Access, rectify, restrict, deletion
Contact: clerk@prolockparishcouncil.gov.uk

6. Data Storage & Security
   - Council-owned systems or approved cloud only
   - Encryption at rest/in transit
   - Devices secured per IT & Digital Policy (passwords, MFA, antivirus)
   - Physical records locked, access restricted

7. Data Subject Rights
   - Access (SAR), rectify, erase, restrict processing, object, portability
   - Consent withdrawal
   - Requests handled by Clerk within statutory timelines (usually 1 month)

8. Data Sharing & Third Parties
   - Only lawful, necessary sharing
   - All processors must sign Data Processing Agreements
   - Sensitive data must be encrypted or securely transferred

9. Incident & Breach Management
   - Immediate reporting to Data Protection Officer/Clerk
   - Containment, assessment, recovery, ICO notification if required
   - Post-incident review, lessons learned, policy update

10. IT Disaster Recovery Plan
    - Daily incremental backups, weekly full backups to encrypted offsite/cloud
    - Quarterly restore tests
    - Recovery priorities: financial systems (24h), emails (24–48h), governance records (48h), website (72h), staff files (72h)
    - Incident steps: Detection → Containment → Assessment → Recovery → Communication → post-incident review

11. Training & Awareness
    - Annual GDPR and IT security training for staff, volunteers and councillors
    - Covers data protection, phishing, secure handling, reporting

12. Monitoring & Audit
    - Audit logs maintained and reviewed periodically
    - Annual review of policy effectiveness

13. Policy Governance
    - Reviewed annually or when legislation/guidance changes
    - Version control, adoption recorded in Council minutes

14. References & Cross-References
    - IT & Policy (2025): Security, device, email, cloud, backup, and disaster recovery requirements
    - Retention & Disposal Policy (2026): All retention periods, disposal methods, and legal compliance

Dated: 13th May 2026

---	---
Duncan McCanlis	Johnathan Jones
Chair	Clerk & Responsible Financial Officer