The Cirl Bunting is the UK's rarest farmland bird. The entire breeding population is found between Exeter and Plymouth.

Coffinswell Parish Council

Serving the Communities of

Coffinswell & Daccombe

IT & Digital Compliance Policy

1. Introduction

This policy sets out how Coffinswell Parish Council manages its information technology systems, digital communications and electronic data.

It incorporates National Association of Local Councils (NALC) guidance and has been tailored to reflect the size and operational arrangements of the Council.

The Council recognises its responsibilities under:
• AGAR Assertion 10 (Digital and Data Compliance)
• The Data Protection Act 2018 and UK GDPR
• The Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018
• The Transparency Code for Smaller Authorities

Policy Ownership This policy is owned by Coffinswell Parish Council and administered by the Clerk as Responsible Officer for digital governance.

2. Purpose

The purpose of this policy is to:
• Protect Council data and digital assets
• Define acceptable use of Council IT systems
• Reduce risk of cyber incident
• Ensure compliance with statutory obligations
• Provide clear accountability and governance controls

3. Scope

This policy applies to:
• All Councillors
• The Clerk
• Contractors handling Council data
• Any authorised user of Council IT systems

Councillors share responsibility for maintaining good digital security practices when using Council systems or handling Council information.

It covers:
• Council email accounts
• Website and domain
• Cloud storage
• Council-owned devices
• Personal devices used for Council business
• Social media accounts

4. Digital Governance & AGAR Compliance

The Clerk is designated as Digital Lead and is responsible for:
• Maintaining secure digital systems
• Reviewing website compliance annually
• Ensuring required documents are published
• Reviewing backup arrangements annually prior to AGAR submission
This policy supports compliance with AGAR Assertion 10 (Digital and Data Compliance).

5. Domain & Email Management

The Council maintains control of its website domain and hosting arrangements.

The Council is in the process of transitioning to a .gov.uk domain. Upon completion, Councillors will use Council-controlled email addresses.

Email security measures include:
• Strong passwords (NCSC “three random words” method)
• Multi-Factor Authentication (where available)
• Removal of access when Councillors or staff leave office

6. Password & Authentication Standards

• All accounts must use strong passwords.
• Passwords must not be shared.

• MFA must be enabled where available.
• Passwords must not be written down insecurely.
• Administrative credentials must be securely stored.
• Passwords must be changed immediately if compromise is suspected.

7. Equipment & Device Security

Council equipment must:
• Be password protected
• Use supported software
• Have updates enabled
• Have antivirus protection enabled

Portable equipment must not be left unattended in public places or overnight in vehicles and must be reported immediately if lost or stolen.

Where personal devices are used:
• Council email must be accessed via official accounts only
• Devices must use a strong passcode
• Devices must auto-lock after inactivity
• Council data must not be saved to personal cloud storage
• Council data must be deleted when leaving office

8. Backup & Business Continuity

Key Council records (including AGAR, financial records, asset register, minutes and insurance documents) must be stored in secure cloud storage.

The Clerk will:
• Review backup arrangements annually
• Confirm that automatic backups are active
• Periodically verify that data restoration is possible

Critical documents should be stored in more than one secure digital location where reasonably practicable.

9. Website & Accessibility Compliance

The Council website will:
• Publish required governance documents
• Maintain a current Accessibility Statement
• Aim to comply with WCAG 2.2 AA standards

New documents should avoid scanned PDFs where reasonably practicable and use accessible formatting.

Accessibility compliance will be reviewed annually.

10. Monitoring

The Council reserves the right to monitor use of its IT systems where necessary for security, investigation of misuse, or where required by law.

Monitoring will be proportionate and compliant with data protection law. Routine intrusive monitoring is not undertaken.

11. Remote Working

When working remotely:

- Passwords must not be saved on shared/public devices
- Public Wi-Fi should be avoided where possible
- Confidential information must not be visible to others
- Printed documents must be stored securely
- Devices must be secured when unattended

12. Email & Internet Use

Email and internet access are provided for Council business.

Limited personal use is permitted provided it does not interfere with Council duties, breach copyright, access inappropriate material, or bring the Council into disrepute.

13. Social Media

Official social media accounts remain the property of the Council.

Councillors must:

- Not represent personal views as Council policy
- Avoid posting confidential information
- Remain mindful of the Members' Code of Conduct
- Avoid content that may damage the Council's reputation

Login credentials must be retained securely and transferred when roles change.

14. Data Protection

Data protection is governed primarily by the Council's Privacy Policy and Document Retention Policy.

All personal data must be processed lawfully, kept secure, not shared inappropriately, and retained in accordance with the Council's Retention Policy. Data breaches must be reported immediately to the Clerk.

15. Misuse

Serious misuse of Council IT systems may result in removal of system access, referral under the Members' Code of Conduct, or disciplinary action where applicable.

Cyber Incident Reporting

Any suspected cyber incident, data breach, phishing attempt or compromise of Council systems must be reported immediately to the Clerk.

The Clerk will assess whether further action is required including notification to the Information Commissioner's Office (ICO), the Council's website provider, or relevant cyber security authorities.

16. Review

This policy will be reviewed annually in May, prior to AGAR approval.

Adopted: Date: 17th March 2026