

WYCK RISSINGTON PARISH COUNCIL – INFORMATION TECHNOLOGY (IT) POLICY MAY 2026 DRAFT

(Please note this draft policy anticipates the adoption of our newly designed website and email addresses in full at the Council meeting)

1. Purpose and Scope

This policy outlines the acceptable use of IT equipment, software, and systems to ensure the security, integrity, and legal compliance of Council data.

This policy applies to all Councillors, the Clerk, and any employees, contractors, and volunteers who access Council information or systems.

2. Official Email & Communication

To comply with proper practices and GDPR, personal email accounts should not be used for official Council business.

Official Accounts: All Council business must be conducted using only the official Council email addresses provided (ending in **@wyckrissingtonparishcouncil.gov.uk**).

3. Device Security

Whether using Council-issued laptops or personal devices to access Council data, the following standards apply:

Passwords: All devices accessing Council email or files should be protected by a strong password or biometric lock.

Updates: Devices should run a currently supported operating system with native security features and automatic updates enabled.

Exit Protocol: Upon ceasing to be a Councillor or employee, all access to Council systems will be revoked and any Council-related data must be deleted from personal devices.

4. Data Storage & Protection

Location: Council documents will only be permanently stored on the Council's hosted cloud website storage.

Data Retention: Emails and documents will be retained or deleted in accordance with the Council's policy for Management and Publication of Information.

5. Website and Social Media

Accessibility: Please see the Council's Accessibility Statement for compliance details regarding the Council's website.

The Council does not have any official social media sites and does not conduct its business on social media. The Clerk participates in the Wyck Rissington WhatsApp Group for dissemination of information only. Any direct requests to the Council should be made by email.

6. Incident Reporting

Any suspected data breach, lost device, or unauthorised access must be reported to the Clerk immediately (within 24 hours). The Clerk will assess if the breach requires reporting to the Information Commissioner's Office (ICO) within 72 hours.