

Roydon Parish Council

Information Technology Policy

Effective Date: January 2026
Review Body: Parish Council
Next Review: January 2027

1. Introduction

Roydon Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications. This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, staff, and authorised users.

2. Scope

This policy applies to all individuals who access or use the Council's IT resources, including computers, networks, software, mobile devices, data, and email accounts. This includes councillors, employees, volunteers, and contractors.

The policy sets out how all users must conduct Council business securely, responsibly, and in compliance with legal and regulatory requirements, including the UK GDPR, Data Protection Act 2018, and Freedom of Information Act 2000.

3. Acceptable Use of IT Resources

The Council's IT resources and email accounts are to be used for official Council-related activities and tasks.

- Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy
- All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content
- Users must not access, distribute, or store illegal or offensive material

4. Device and Software Usage

- Council-authorised devices, software, and applications will be provided for work-related tasks where possible
- Unauthorised installation of software on Council-provided devices is strictly prohibited due to security concerns
- Personal software installation is not permitted without explicit written approval from the Parish Clerk
- Personal disks, USB sticks, and external storage devices cannot be used on Council computers without prior approval from the Parish Clerk

5. Data Management and Security

All sensitive and confidential Council data must be:

- Stored and transmitted only via Council-managed systems with encryption in transit and at rest
- Handled in accordance with the Council's Data Protection Policy and UK GDPR requirements

- Backed up regularly to prevent data loss
- Destroyed securely using approved methods in accordance with the Council's retention schedule

Personal devices may not be used to store Council data unless explicitly authorised in writing by the Parish Clerk and the data is encrypted.

6. Network and Internet Usage

The Council's network and internet connections should be used responsibly and efficiently for official purposes only.

- Downloading and sharing copyrighted material without proper authorisation is prohibited
- Users must comply with the Council's Communications Policy when using social media platforms for Council business
- Excessive use of bandwidth for non-work purposes is prohibited

7. Email Communication

Council email accounts are for official communication only. Users must:

- Use professional, courteous, and respectful tone in all communications
- Not send confidential or sensitive information via email unless encrypted
- Use Blind Carbon Copy (BCC) when communicating externally with multiple recipients to protect personal data and comply with UK GDPR
- Exercise caution with attachments and links to avoid phishing and malware
- Verify the source of emails before opening attachments or clicking links

Personal email and messaging apps must not be used to conduct Council business. Instant messaging apps (WhatsApp, Signal, iMessage, etc.) must not be used for decisions, instructions, casework, or contract negotiations. Any substantive matters agreed verbally or by text must be confirmed by Council email within one working day.

Council email ownership: All Council-issued email addresses and related data are the property of the Council. Councillors and staff act on behalf of the Council when using these accounts and must comply with this policy, the Data Protection Policy, and the Freedom of Information Act. All correspondence forms part of the Council's official record and may be disclosable under Freedom of Information or audit inspection.

Departing councillors: When leaving office, email access will be withdrawn, the mailbox will be securely deleted by the IT provider, and departing councillors must not retain or continue to use personal data obtained through their role.

8. Password and Account Security

Council users are responsible for maintaining the security of their accounts and passwords.

- Passwords should be strong and contain a combination of letters, numbers, and special characters
- Passwords must not be shared with others
- Do not reuse passwords across different accounts
- Enable multi-factor authentication (MFA) where available
- Change passwords only when there is a suspected breach or compromise
- Lock computers when leaving your desk to prevent unauthorised access

9. Mobile Devices and Remote Work

- Mobile devices provided by the Council must be secured with passcodes and/or biometric authentication
- When working remotely, users must follow the same security practices as if in the office
- Use secure connections (VPN) when accessing Council systems remotely
- Do not store sensitive Council data on personal mobile devices unless authorised and encrypted

10. Email Monitoring

The Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act 2018 and UK GDPR.

11. Retention and Archiving

Emails should be retained and archived in accordance with legal and regulatory requirements and the Council's retention schedule. Users should:

- Regularly review and delete unnecessary emails to maintain an organised inbox
- Retain emails relating to Council business in accordance with the retention schedule
- Archive completed project-related emails as directed by the Parish Clerk

12. Reporting Security Incidents

All suspected security breaches, data protection incidents, or IT-related incidents should be reported immediately to the Parish Clerk for investigation and resolution. This includes:

- Phishing emails or suspicious messages
- Potential malware or security threats
- Unauthorised access attempts
- Lost or stolen devices

13. Training and Awareness

The Council will provide appropriate training and guidance to all users to support compliance with this policy. Users are expected to complete any training provided and remain aware of security best practices.

14. Compliance and Consequences

Breach of this policy may result in disciplinary action, including:

- Formal warnings
- Suspension of IT access
- Disciplinary proceedings
- Potential termination of employment
- Legal action if criminal activity is involved

15. Policy Review

This policy will be reviewed annually or when significant changes to IT infrastructure, regulations, or working practices occur.

Policy approved by: Roydon Parish Council

Date of approval: January 2026

Signed: _____ (Council Chair)