Purley on Thames Parish Council

PURLEY ON THAMES PARISH COUNCIL IT POLICY

Introduction

Digital working, the use of IT systems, and the handling of data are integral to parish council operations. The Council recognises that effective information governance and cyber security are essential to:

- Protect personal data in accordance with the UK GDPR and Data Protection Act 2018
- Comply with the Freedom of Information Act 2000
- Meet Cyber Insurance requirements

Purpose

This policy establishes clear parameters for how councillors, staff, and authorised users use council provided IT systems or equipment in the course of their duties.

This policy aims to:

- Set expectations for acceptable use of equipment and systems
- Raise awareness of cyber and data security risks
- Safeguard the council's data and digital assets
- Clarify what constitutes acceptable and unacceptable use
- Outline the consequences of policy breaches

Scope

This policy applies to:

- All councillors
- All staff
- Any authorised contractor or user accessing Council systems

It applies regardless of working location or pattern, including home-based, office-based or work on a flexible or part-time basis.

Monitoring

The Council reserves the right to monitor the use of its IT equipment and systems where there is a legitimate and proportionate reason to do so.

Monitoring may take place in order:

- Protect against cyber threats
- Investigate suspected misconduct
- Maintain system security and integrity
- Comply with legal obligations
- Meet Cyber Insurance requirements

Monitoring will comply with data protection and privacy legislation.

Adopted: 10 March 2026

Acceptable Use of IT Systems

Council IT systems are provided primarily for legitimate Council business.

Users must:

- Use IT systems provided by the Council for official Council business
- Ensure personal use does not interfere with duties
- Respect copyright and intellectual rights
- Not use Council systems for unlawful, defamatory or offensive activities
- Not access inappropriate or illegal content

Device and Software Usage

Purley on Thames Parish Council provides:

- Council-owned laptops to all office staff
- Council-owned mobile phones to two staff members
- Microsoft 365 email accounts to all councillors and staff

All devices must:

- Be secured with a password, PIN, fingerprint or facial recognition
- Be locked when unattended
- Not be used by unauthorised individuals
- Be treated with reasonable care
- Have only authorised software installed

Lost or stolen devices must be reported to the Parish Clerk.

Use of Personal Devices (BYOD)

Councillors and authorised users may use personal devices for Council purposes (e.g. council email account and calendar access), provided security standards are maintained.

Personal devices used for Council work must:

- Be secured with a strong PIN/password
- Be kept updated with operating system and security patches
- Not be modified from their standard secure operating system

Users must:

- Keep Council and personal data separate where possible
- Avoid permanently storing sensitive Council documents locally on personal devices.

Councillors, staff and other authorised users remain personally responsible for their own devices.

Device Management and Security

All sensitive and confidential Purley on Thames Parish Council data must be handled securely.

Users must:

- Store and transmit data securely using approved methods.
- Ensure regular data backups to minimise the risk of data loss
- Dispose of data securely when no longer required
- Follow the Council's Retention Schedule

Network and Internet Usage

Council network and internet connections must be used responsibly.

Users must not:

- Download or share copyrighted material without authorisation
- Install unauthorised software
- Access inappropriate or illegal content

Email and Communication

Council-issued email accounts must be used for all official Council business.

Users must:

- Not forward Council emails to personal email accounts
- Not use personal email accounts for Council work
- Ensure email correspondence is professional and respectful.
- Use BCC where appropriate when emailing groups externally
- Report phishing or suspicious emails immediately to the Clerk

All official communications may be subject to disclosure under the Freedom of Information Act 2000 and Data Protection legislation.

Email accounts will be deactivated when councillors or staff leave the Council.

Password and Account Security

Strong account security is essential to protect Council systems.

Users must:

- Use strong passwords
- Not share passwords with others.
- Enable Multi-Factor Authentication (MFA) where available
- Change passwords immediately if compromise is suspected

Users are responsible for maintaining the confidentiality of their login credentials.

Email Monitoring

Purley on Thames Parish Council reserves the right to monitor email communications where necessary and proportionate to ensure compliance with this policy and relevant legislation.

Monitoring will be conducted in accordance with UK GDPR and the Data Protection Act 2018.

Remote working

When working remotely, users must follow the same security standards as in the office.
Users must:

- Secure devices with passcodes and/or biometric authentication
- Avoid unsecured public Wi-Fi where possible
- Keep devices and papers secure
- Store documents within approved Council systems

Retention and Achiving

Emails and electronic records must be retained in accordance with the Council's adopted Retention Schedule and relevant legislation.

Reporting Security Incidents

All suspected security breaches or incidents must be reported immediately to the Parish Clerk

This includes:

- Lost or stolen devices
- Phishing attempts
- Suspected malware
- Accidental disclosure of personal data

Where a personal data breach is suspected, the Clerk will assess whether notification to the Information Commissioner's Office (ICO) is required within 72 hours in accordance with UK GDPR.

Training and Awareness

The Council will provide appropriate resources and guidance to educate users about:

- IT security best practice
- Phishing and cyber threats
- Data protection responsibilities
- Technology updates and system changes

Compliance and Consequences

Failure to comply with this policy may result in:

- Suspension or removal of IT access
- Disciplinary action (for employees)
- Referral to the Monitoring Officer (for councillors)

Serious breaches may constitute gross misconduct.

Policy Review

This policy will be reviewed annually or when significant changes occur.