IT (Information Technology) Security policy

1. Introduction

Yalding Parish Council (YPC) recognises the importance of maintaining secure and reliable information technology systems to support its business operations, communications and statutory responsibilities. This policy sets out the standards, responsibilities and procedures for the appropriate and secure use of the Council's IT resources.

All users must only access systems and data they are authorised to use, not disclose Council data to unauthorised persons, comply with all relevant Council policies and UK legislation, ensure the security of Council data.

2. Scope

This policy applies to all Councillors, employees, volunteers, contractors and any other individuals who access or use YPC's IT systems, devices, networks, software, email accounts or data.

3. Acceptable Use

Council IT resources must be used primarily for official Council business. Limited personal use is permitted provided it does not interfere with Council duties, does not incur cost to The Council, and does not breach this or any other Council policy. Users must act lawfully, ethically and responsibly at all times.

4. Data Security and Handling

All Council data, including personal data, must be stored, accessed, transmitted and disposed of securely. Users must follow The Council's Data Protection Policy and Records Retention Policy, ensure confidential or sensitive information is encrypted when sent electronically, use only approved storage locations for Council data, and ensure secure deletion of data when no longer required. Personal devices used to access Council information must apply the same level of security as Council owned equipment.

5. Devices, Software and Updates

All devices used for Council business must be protected by passwords, PINs or biometric authentication, kept updated with current security patches, and protected

by anti-virus or anti-malware software where applicable. Only authorised software may be installed on Council devices.

If a device is shared with anyone else, ensure separate password protected user accounts are used and that Council information is only accessible from your own account.

The Council's electronic records will be backed up regularly using secure, approved methods such as a portable hard dive or Cloud storage. Officers must ensure that important files are stored in locations included in the Council's backup process.

6. Network and Internet Use

Council internet and network access must be used responsibly. Users must not download or share copyrighted material without permission, access inappropriate or illegal content or attempt to bypass security controls or firewalls.

7. Email Use

Council issued email accounts must be used for all official Council correspondence.

Councillors may use their personal email accounts to receive and reply to routine Council correspondence. All formal or official communications on behalf of the Council are issued by The Clerk, Deputy Clerk or Chairman using the Council's .gov.uk email addresses. @yaldingparishcouncil.gov.uk email addresses are provided strictly for official Council business. They must not be used for personal correspondence or non-Council activity

Councillors must ensure that any Council related emails held on personal devices are handled securely and retained only where absolutely necessary for Council business, in accordance with The Council's Records Retention Policy. Councillors must not share any personal data obtained through Council correspondence and must provide any relevant emails to the Clerk if required for Freedom of Information or Subject Access Requests.

When emailing multiple recipients, users must use Blind Carbon Copy (BCC) to prevent disclosure of personal email addresses. CC must only be used where all recipients already have a legitimate need to see each other's contact details.

When using email for Council business, users must maintain a professional tone, be alert to phishing and suspicious links and avoid sending confidential information unless it is encrypted.

8. Password and Account Security

Users are responsible for keeping their accounts secure. Passwords must be strong and unique, not shared and changed if compromised. Multi-factor authentication (MFA) is used for high-risk systems such as online banking and must be enabled wherever it is provided or required. Where MFA is not available, users must ensure that passwords and devices are protected to an equivalent standard.

9. **Remote Working and Mobile Devices**

When working remotely or using mobile devices, users must protect devices from unauthorised access, avoid unsecured public Wi-Fi and ensure screens cannot be overlooked in public places.

When attending meetings or working in public or shared spaces, users must keep devices with them at all times, ensure screens are not visible to others and avoid leaving laptops, tablets or phones unattended.

10. **Monitoring**

The Council may monitor the use of its IT systems, including email, to ensure compliance with this policy and with legal obligations. Monitoring will be carried out in accordance with UK GDPR and the Data Protection Act 2018.

11. **Email and Data Retention**

Emails and electronic records must be retained, archived or deleted in accordance with The Council's Records Retention Policy. Users should regularly review and delete non-essential emails.

12. **Security Incidents**

Any suspected or actual security breach, including loss of devices, unauthorised access, malware or data loss, must be reported immediately to The Clerk (or Chairman in their absence). Incidents will be investigated and managed in line with The Council's Data Breach Procedure

13. **Use of Artificial Intelligence (AI) Tools**

AI tools may be used to support drafting, research and productivity, provided they are used responsibly and in accordance with UK GDPR and this IT Security Policy.

Users must ensure that:

- No personal data, confidential information or sensitive material is entered into public AI tools.
- AI tools are used only for non-confidential drafting or administrative support.
- Outputs from AI tools are checked for accuracy and do not replace professional judgement.
- AI must not be used to make decisions about individuals or to process personal data.
- AI outputs must be reviewed for accuracy and must not be relied upon without verification.

14. **Training and Awareness**

The Council will provide periodic training and guidance on IT security, data protection and safe email practices. The Council has a Cyber Security Good Practice Guide for Councillors, Officers and Volunteers.

15. **Compliance**

Failure to comply with this policy may result in withdrawal of IT access, disciplinary action where applicable or reporting to relevant authorities in serious cases.

16. **Contacts**

For IT-related queries or to report a security incident, contact: The Clerk to Yalding Parish Council.

Adopted on 03 March 2026

To be reviewed annually at the Annual Parish Council Meeting (see minutes of that meeting) or sooner if required due to legislative or technological changes.