CYBER SECURITY GOOD PRACTICE GUIDE
FOR COUNCILLORS, OFFICERS AND VOLUNTEERS

Yalding Parish Council (YPC) relies on technology to manage information, communicate effectively and deliver services. Everyone who handles Council information has a responsibility to keep that information secure and to help prevent cyber incidents. This guide provides practical, easy to follow steps to help protect Council systems, data and devices. It supports the Council's IT Security Policy and Data Protection Policy.

1. Protecting Council Information

All users of Council electronic data must take reasonable steps to keep that data secure. This includes:

- Handling emails carefully
- Protecting devices
- Avoiding suspicious links or downloads
- Reporting concerns promptly

Even if you do not have a Council issued device, you may still handle Council information and must follow these good practice guidelines.

2. Email Safety

Most cyber incidents begin with a malicious email.

To reduce the risk:

- Avoid opening attachments or clicking links unless you are confident they are genuine.

- Be cautious of vague or unusual messages such as “watch this video” or “urgent invoice attached.”
- Check the sender’s email address carefully, look for spelling errors or unusual domains.
- Watch for poor grammar, unexpected urgency or anything that feels wrong.

If unsure, contact the Clerk before opening the message. Formal and official Council emails should only be sent from a @yaldingparishcouncil.gov.uk email address. Councillors should delete routine Council emails once dealt with.

@yaldingparishcouncil.gov.uk email addresses are provided strictly for official Council business. They must not be used for personal correspondence or non-Council activity.

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

3. Password Good Practice

Strong passwords help protect Council information.

Users should:

- Use passwords that are long, unique and difficult to guess.
- Avoid using personal information such as birthdays or pet names.
- Store passwords securely, do not leave them written down or visible.
- Change passwords immediately if you believe they may have been compromised.
- Where available, enable multi-factor authentication (MFA) for added protection.

4. Protecting Devices

Whether using a Council device or a personal device for Council work:

- Ensure devices have up to date antivirus or anti-malware protection.
- Keep operating systems and software updated.
- Lock your screen when leaving your device unattended.
- Avoid using public or unsecured Wi-Fi for Council business.
- If you share a device with anyone else, ensure separate password protected user accounts are used and that Council information is only accessible from your own account.
- If a device used for Council work is lost or stolen, report it immediately to The Clerk.

5. Safe Browsing and Downloads

To reduce the risk of malware:

- Avoid accessing suspicious or untrusted websites.
- Do not download software, apps or files unless necessary and from reputable sources.
- Be cautious of pop-ups offering prizes, warnings or downloads.

6. Reporting Concerns

Report the following to the Clerk as soon as possible:

- Suspicious emails
- Suspected scams
- Privacy breaches
- Hacking attempts
- Lost or stolen devices
- Unusual system behaviour
- Anything that “does not look right”

Early reporting helps prevent further damage.

7. Data Handling and Storage

To protect Council information:

- Only keep emails and documents that are necessary for Council business.
- Delete routine or duplicate information once no longer needed.
- Back up important electronic files regularly (officers only).
- Review stored data periodically and remove anything unnecessary.
- Follow The Council’s Records Retention Policy for how long information should be kept.

8. Good Practice for Councillors

Councillors who do not use Council issued devices should:

- Delete routine Council emails once dealt with
- Avoid storing personal data about residents
- Forward anything relevant to Freedom of information and Subject Access Request to The Clerk
- Keep their own devices secure and updated
- Avoid mixing Council files with personal files

Adopted on 3 March 2026

To be reviewed annually at the Annual Parish Council Meeting (see minutes of that meeting).