# Hanborough Parish Council

# IT and Bring Your Own Device (BYOD) Policy

*Adopted 13th October 2026*

| Item | Details |
|---|---|
| Version | v3 – simplified version for adoption |
| Adopted by council | 13/10/2026 2026/10/176-110 |
| Owner | Clerk / Proper Officer, on behalf of the Council |
| Applies to | Councillors, employees, contractors and authorised volunteers |
| Review | Every two years, or sooner if something significant changes |

*You do not need to be an IT expert to follow this policy. If you are unsure about anything, ask the Clerk. Technical words are explained in Appendix C.*

## This policy at a glance: ten golden rules

1. Use your council email address for council business, not your personal email.
2. Keep council documents in the council's shared storage, not only on your own device.
3. Lock your phone, tablet and computer with a PIN, password, fingerprint or face.
4. Install updates when your device asks you to.
5. Use a different, strong password for council accounts and turn on two-step login.
6. Never make a payment or change bank details because of an email or message alone. Phone a number you already know to check first.
7. Use WhatsApp only for arranging things. Never use it for decisions, personal details or confidential matters.
8. Only post on behalf of the council if you are authorised. Make clear when you are speaking personally.
9. Never put personal or confidential council information into AI tools such as ChatGPT, and check everything they produce.
10. If something goes wrong, tell the Clerk the same day. You will not be blamed for reporting a genuine mistake.

# The policy

## 1. Why we have this policy

This policy explains how to use email, devices, the internet, messaging apps, social media, the council website and AI tools safely for council business. It protects residents' personal information, public money and the council's reputation. It recognises that most councillors are volunteers using their own phones and computers.

## 2. Who and what it covers

It applies to councillors, staff, contractors and volunteers who do council business. It covers:

- council equipment, and your own devices when you use them for council business;
- council email, shared storage and other council systems;
- the council website and council social media accounts;
- WhatsApp and other messaging apps used for council business;
- AI tools used for council business.

Read it alongside the Members' Code of Conduct (councillors), your terms of employment (staff), and the council's data protection and records policies.

## 3. Council email and documents

- Use your council email address for all council business. If you ever have to use personal email in an emergency, forward the message to your council email and then delete it from your personal account.
- Do not set up automatic forwarding from council email to a personal email account.
- Save council documents in the council's shared storage [insert name, e.g. Microsoft 365], not only on your own device, a USB stick or a personal account such as iCloud, Google Drive or Dropbox.
- If you download a council document to your device, delete it once you have finished with it.
- Use BCC when emailing several members of the public, so their email addresses are not shared with each other.

## 4. Using your own phone, tablet or computer

You may use your own device for council business if it meets these basic standards. Appendix A is a simple checklist, and the Clerk can help you check.

- It still receives security updates from the manufacturer, and you install updates when asked.
- It is locked with a PIN, password, fingerprint or face, and locks itself after no more than 15 minutes.
- It has not been 'jailbroken' or 'rooted' (altered to remove the manufacturer's security).
- Family members or others who use the device cannot open your council email or documents. On a shared computer, use your own login.
- On a laptop or desktop, the built-in virus protection is switched on.
- If it is lost, stolen, or you think it has been hacked, stop using it for council business and tell the Clerk.

### When you are out and about

- Make sure others cannot see your screen or papers, and never leave devices unattended.

- Do not use public or shared computers (for example in a library) for council business.
- Do not do council banking on public Wi-Fi.

### Your privacy

The council will not inspect your personal device or look at your personal content. If there is a security problem, or when you leave, you will be asked to remove council email and documents from your device and to help with reasonable steps limited to council information.

### Council-owned equipment

Equipment provided by the council belongs to the council. Use it mainly for council business, look after it, report any loss or damage, and return it when you leave.

## 5. Passwords and two-step login

- Use a strong password for each council account that you do not use anywhere else. Three random words joined together is an easy way to make one.
- Never share your council password with anyone, including family or other councillors. The Clerk will never ask for it.
- Turn on two-step login wherever it is offered. As well as your password, you enter a code from your phone. It must be used for council email, banking, the website and social media accounts.
- A password manager, including the one built into your phone or browser, is a safe way to store passwords.
- Change your password straight away if you think someone else knows it.

## 6. Scams, payments and banking

- Be wary of unexpected emails or messages that are urgent, or ask you to click a link, open an attachment, log in, pay, or change bank details, even if they seem to come from someone you know.
- Never make a payment or change a supplier's bank details based only on an email or message. Check by phoning a number you already know.
- Only authorised people may use council online banking, and they must use two-step login.
- If you think you have clicked on something suspicious, tell the Clerk straight away.

## 7. WhatsApp and other messaging apps

Messaging apps such as WhatsApp are fine for arranging meetings, reminders and practical updates, or for letting people know an email has been sent. They must not be used for:

- making, or appearing to make, council decisions, or debating agenda items in advance. Decisions are made at council meetings;
- personal details about residents, staff or anyone else, or confidential council matters;
- anything you would not be comfortable seeing made public. Messages about council business can be requested under freedom of information law, even if they are on your personal phone.

Also:

- any council WhatsApp group is run by the Clerk (or a person the council nominates), who removes people when they leave;
- do not use disappearing messages for council business;
- if a message contains something the council needs to keep, such as a complaint, forward it to the Clerk by email;

- the Code of Conduct applies to messages just as it does to anything said in person;
- turn on two-step verification in WhatsApp and never share the six-digit code it sends you.

## 8. The council website and social media

### Council website and council social media accounts

- They belong to the council. They must be registered in the council's name using a council email address, and at least two authorised people (normally the Clerk and one other) must hold the logins.
- Only authorised people may post or change content. Content must be accurate, politically neutral and reflect council decisions, with extra care before elections.
- Do not publish personal details, or photos of identifiable people (especially children), without consent.
- The Clerk will make sure the website is kept up to date and backed up, has a privacy notice, meets transparency and accessibility requirements, and that the web address and hosting are renewed on time.
- Complaints or information requests received online must be passed to the Clerk.

### Your own social media and community groups

- Make clear when you are speaking personally and not for the council.
- Councillors: the Code of Conduct applies whenever you are, or appear to be, acting as a councillor, including online and in village Facebook or WhatsApp groups.
- Do not share confidential information or announce decisions before they have been made.
- Do not show you have already made up your mind on something the council has yet to decide, especially planning applications.
- Staff should follow their employment terms when posting about anything connected with the council.

## 9. AI tools

AI tools such as ChatGPT, Microsoft Copilot or Google Gemini can help draft and summarise text. However, they can get things wrong, and some keep what you type into them.

- Only use AI tools the Clerk has approved for council work.
- Never type or upload personal details, confidential council information or passwords.
- Always check what AI produces. It can invent facts, figures and laws, and you are responsible for anything you use.
- AI must never make council decisions.
- Do not use AI recording or note-taking tools in meetings without the Clerk's approval and telling everyone present, and never in the confidential part of a meeting.
- Do not use AI to create fake or misleading images, audio or video, or to pretend to be someone else.
- Be alert: scammers use AI to fake voices and messages from people you know.

## 10. If something goes wrong

Tell the Clerk the same day if:

- a device with council email or documents is lost or stolen;

- you think someone has got into your council account, or you clicked something suspicious;
- personal or confidential information has gone to the wrong person, a group, online, or into an AI tool;
- the council website or a social media account has been hacked;
- you receive a suspicious request for payment or a change of bank details.

Appendix B explains what to do straight away. The Clerk, with the Chair where needed, will deal with the problem and decide whether it must be reported to the Information Commissioner's Office (within 72 hours where required). Nobody will be criticised for reporting a genuine mistake promptly.

## 11. Joining and leaving

- New users will be given the access they need and a copy of this policy, and asked to sign the declaration below.
- When someone leaves, the Clerk will remove their access to council email, systems, the website, social media accounts and messaging groups, and change any shared passwords.
- Leavers must return council equipment, delete council documents from their own devices and personal accounts, and pass any council records to the Clerk.

## 12. Monitoring

The council may check records held in its own systems, such as council email and website records, where this is necessary to keep them secure, investigate a problem or meet legal duties. It will not monitor your personal devices or personal accounts.

## 13. If this policy is not followed

The aim is to fix problems, not to blame people. For staff, serious or repeated breaches may be dealt with under employment procedures. For councillors, access to council systems may be withdrawn, and the matter may be considered under the Members' Code of Conduct or referred to the Monitoring Officer.

## 14. Review

This policy will be reviewed every two years, or sooner after a serious incident, a change of council systems, or a change in law, guidance or technology (including AI).

## Appendix A – Quick checklist

Before using your own device for council business, you should be able to answer yes to each of these.

| Check | I can say yes to this |
|---|---|
| Updates | My device still gets security updates, and I install them when asked. |
| Screen lock | My device has a PIN, password, fingerprint or face lock and locks itself after a few minutes. |
| Privacy | Nobody else who uses my device can open my council email or documents. |
| Passwords | My council passwords are strong, not used anywhere else, and not shared. |
| Two-step login | Two-step login is turned on for my council accounts and WhatsApp. |
| Council email | I use my council email address for council business. |
| Storage | I keep council documents in the council's shared storage and delete downloaded copies. |
| Scams | I never pay or change bank details on the strength of an email or message alone. |
| WhatsApp | I use messaging apps only for arrangements, never for decisions or personal details. |
| Social media | I make clear when I am speaking personally and keep council matters confidential. |
| AI tools | I only use approved AI tools, never enter personal or confidential information, and check the results. |
| Reporting | I know to tell the Clerk the same day if something goes wrong. |
| Leaving | I will return council equipment and delete council information when my role ends. |

## Appendix B – What to do if something goes wrong

In every case, tell the Clerk the same day.

| What happened | What to do straight away |
|---|---|
| Lost or stolen device | Change your council passwords from another device. Use "Find my phone" (or similar) to lock or wipe it if you can. |
| Clicked a suspicious link or attachment | Disconnect from the internet if you think a virus may be involved. Do not delete the message. Change passwords from another device if the Clerk advises. |
| Account may have been hacked | Change the password and check two-step login is on. Warn contacts if strange messages may have been sent from your account. |
| Information sent to the wrong person, posted, or put into an AI tool | Delete it where you can and ask recipients to delete it. Note what was shared, where and when. |
| Suspicious request for payment, bank changes, gift cards or codes | Do not pay, reply or share any code. Check with the person on a number you already know. |
| Council website or social media hacked | Take screenshots, then change passwords and check two-step login from a trusted device. |

## Appendix C – Jargon buster

| Term | What it means |
|---|---|
| AI tool | Software such as ChatGPT or Copilot that writes or summarises text, or creates images, when you type a request. |
| BCC | "Blind copy" in email. People in the BCC box cannot see each other's email addresses. |
| BYOD | "Bring your own device": using your own phone, tablet or computer for council business. |
| Cloud / shared storage | Storing documents online (for example Microsoft 365) so they are safe and available even if a device is lost. |
| Jailbroken / rooted | A phone or tablet altered to remove the manufacturer's security controls. |
| Password manager | An app, or a feature built into your phone or browser, that safely remembers your passwords. |
| Personal data | Any information about an identifiable living person, such as a name, address, phone number or photo. |
| Phishing | Fake emails or messages designed to trick you into clicking a link, giving a password or making a payment. |
| Security updates | Fixes sent by the maker of your device or software to close security holes. |
| Two-step login (MFA) | Logging in with your password plus a code from your phone, so a stolen password alone is not enough. |