Hanborough Parish Council

Information Technology and BYOD Policy

Simple, practical draft for paid staff and volunteer councillors

Item	Details
Status	Draft for review and adoption
Adopted by council	[Insert date]
Owner	Clerk / Proper Officer, on behalf of the Council
Applies to	Councillors, employees, contractors and authorised volunteers
Review cycle	Every two years, or sooner after a cyber incident or major system change

This draft is designed for a small parish council with simple IT needs and BYOD use. It should be checked against the council's employment, data protection, records management and social media policies before adoption.

Review of the example policy

The example policy contains many useful points, including MFA, strong passwords, device locks, secure storage, and reporting lost devices. However, it reads more like a staff handbook for an organisation with managed IT infrastructure than a practical policy for a small parish council where many users are volunteer councillors using their own devices.

Recommended changes before adoption

Issue	Recommended revision
Make it shorter	The example is around 12 pages and contains repeated headings, detailed social media rules and workplace provisions that may distract from the essentials.
Separate staff and councillor consequences	Employees are subject to employment procedures. Councillors are normally handled through council access controls, the Members' Code of Conduct, and where relevant the Monitoring Officer.
Narrow intrusive BYOD wording	Avoid broad rights to inspect or take possession of personal devices. The council should normally require deletion of council data, withdrawal of account access, and cooperation in a specific incident, rather than full access to personal content.
Make monitoring proportionate	Only state monitoring that the council can actually do, such as logs from council email, cloud services, website administration, finance systems or council-owned devices.
Prefer council accounts and cloud storage	Council business should be done through council email/accounts. Avoid storing the only copy of council records on a personal device.
Keep social media brief	Use a short cross-reference to the Code of Conduct and any Social Media Policy rather than a long social media policy inside the IT policy.
Create a simple BYOD checklist	Councillors and staff should be able to understand the minimum requirements in one page.

Core standard recommended for this council

- Use council email and council-approved cloud storage for council business.
- Require MFA on council email, finance, website, cloud storage and administrator accounts wherever available.
- Require supported and updated devices only; no unsupported operating systems, rooted or jailbroken phones, or shared accounts.
- Require a screen lock, password/PIN/biometric unlock, automatic locking, and encryption where available.
- Do not use personal email or personal cloud storage for council records except in a genuine emergency, and then move the record into the council system as soon as possible.
- Report lost devices, phishing, unauthorised access, or accidental disclosure immediately to the Clerk.
- Remove access and delete local council data when a councillor, employee or authorised user leaves.

Information Technology and BYOD Policy

1. Purpose

This policy sets simple rules for using information technology for council business. It aims to protect council information, personal data, public funds and the reputation of the council, while recognising that many councillors are volunteers and may reasonably use their own devices.

2. Who this policy applies to

This policy applies to all councillors, employees, contractors and authorised volunteers who use council information, council email, council systems, council-owned equipment or personal devices for council business.

For employees, breach of this policy may be dealt with under the council's employment procedures. For councillors, breach of this policy may result in withdrawal of access to council systems and may be considered under the Members' Code of Conduct or referred to the Monitoring Officer where appropriate.

3. Simple principles

- Use council accounts for council business. Do not use personal email for routine council business.
- Keep council information separate from personal information wherever possible.
- Only access the information needed for your council role.
- Protect your device, account and password as if they contained confidential council papers.
- Be cautious with links, attachments, payment requests and unexpected changes of bank details.
- Report security concerns quickly. No one will be criticised for reporting a genuine mistake promptly.

4. Council accounts and approved systems

- The council will provide or approve the email accounts and systems to be used for council business.
- Council business must normally be conducted through council email addresses and council-approved storage or document systems.
- Council documents must not be stored permanently in personal email, personal cloud storage, messaging apps or removable storage unless specifically authorised by the Clerk.
- Shared council accounts should be avoided where possible. Where a shared account is unavoidable, access must be limited to authorised users and credentials must be stored securely.
- Administrator access must be limited to those who need it and must not be used for ordinary email or web browsing.

5. Bring Your Own Device (BYOD)

The council permits councillors, employees and authorised users to use personal devices for council business, provided the requirements below are followed. BYOD is a privilege, not an unrestricted right. The council may withdraw access if there is a security concern or if this policy is not followed.

5.1 Minimum requirements for all personal devices

- The device must use a currently supported operating system and must receive security updates.
- Automatic updates must be enabled where available for the operating system, browser and key applications.
- The device must be protected by a PIN, password, passphrase, fingerprint or face unlock.

- The device must lock automatically after a short period of inactivity. A maximum of 15 minutes is recommended.
- Full-device encryption should be enabled where available. Most modern phones, tablets and laptops support this.
- The device must not be rooted, jailbroken, or configured to bypass normal security controls.
- The device must not be shared in a way that allows family members, friends or others to view council email or documents.
- A firewall must be enabled on laptops and desktop computers where available.
- Malware protection must be active and kept up to date where the operating system supports it.
- The device must not be used for council business if the user knows or suspects it is infected, compromised, stolen, lost or no longer receiving updates.

5.2 What council data may be stored on personal devices

- Users should work in council-approved cloud systems wherever possible rather than downloading files locally.
- The only copy of a council record must never be kept on a personal device.
- Confidential, financial, employment, legal or sensitive personal data should not be stored locally on a personal device unless there is a clear council need and the file is protected appropriately.
- Where documents are downloaded temporarily, they should be deleted from the device once no longer needed and retained in the council system if they are council records.
- Personal cloud backup of council documents should be avoided where possible. Users should not deliberately upload council documents to personal cloud services.

5.3 Privacy and council access to personal devices

The council does not have a general right to inspect a user's personal device or personal content. However, users must cooperate with reasonable steps needed to protect council information, investigate a suspected security incident, respond to a legal obligation, or remove council data when access ends. Such steps should be limited to council data and council accounts wherever possible.

6. Passwords and multi-factor authentication

- All council accounts must use strong, unique passwords or passphrases. Users are encouraged to use three or more random words or a password manager to create strong passwords.
- Passwords must not be reused from personal accounts or other services.
- Passwords must not be shared with other councillors, staff, family members or friends.
- MFA must be enabled for council email, cloud storage, finance systems, website administration, social media administration and any administrator account wherever the service supports it.
- Where a password manager is approved by the council, users are encouraged to use it. Administrative and shared credentials must be stored securely and access must be limited.
- Passwords must be changed promptly if compromise is suspected. Routine forced password changes are not required unless there is a specific reason.

7. Email and messaging

- Council email should be used for council business. Personal email should not be used for routine council business.

- Users must be cautious with links, attachments, unexpected payment requests, changes of bank details, urgent messages and requests for personal data.
- Confidential or sensitive material should not be sent to personal email accounts. Where practical, share a link to a council-approved system rather than sending attachments.
- When emailing multiple external recipients, use BCC where appropriate to avoid disclosing email addresses unnecessarily.
- Council business should not be conducted through personal messaging apps unless unavoidable. Any council record created that way should be copied into the council's record system where necessary.
- Users must not set automatic forwarding from council email to personal email unless expressly authorised by the Clerk.

8. Finance systems, banking and payments

- Access to finance systems, online banking and payment authorisation must be limited to authorised users.
- MFA must be used for finance and banking systems wherever available.
- Bank details, payment instructions and supplier changes must be checked using an agreed independent process before payment is made.
- Users must not save finance or banking passwords in a browser unless this has been approved and secured by the council.
- Where possible, finance and banking work should be done from a trusted, updated device on a secure network. Public or shared computers must not be used for council banking.

9. Remote working and public places

- Take reasonable care that council documents and emails cannot be seen by others when working in public or shared spaces.
- Do not leave devices, papers or removable media unattended in public places or vehicles.
- Avoid using public computers for council business. If there is no alternative in an emergency, do not save passwords, log out fully, and do not download council documents.
- Use trusted Wi-Fi where possible. Be cautious when using public Wi-Fi and avoid sensitive work where the connection or device is not trusted.
- Printed council papers must be stored securely and disposed of securely when no longer required.

10. Council-owned equipment

- Council-owned equipment remains the property of the council and must be used primarily for council business.
- The council will keep a simple asset register for council-owned laptops, tablets, phones and other significant IT equipment.
- Users must take reasonable care of council equipment and report loss, theft, damage or suspected compromise promptly.
- Council equipment must not be passed to another person, sold, disposed of, repaired or reconfigured without authorisation.
- Only authorised software and services may be installed or used on council-owned equipment.

11. Backups and records

- Council records should be stored in the council's approved email, finance, website or document system so that they are available to the council if an individual is absent or leaves.
- The Clerk should ensure there is a suitable backup or recovery arrangement for important council documents and records.
- Users must not keep the only copy of council records on personal devices, personal email, USB drives or personal cloud accounts.
- Council records must be retained and deleted in accordance with the council's retention policy and legal obligations.

12. Internet, software and cloud services

- Users must not use council systems for unlawful, fraudulent, discriminatory, harassing, obscene or otherwise inappropriate activity.
- Software, apps and cloud services used for council business must be approved by the Clerk or the council where appropriate.
- Users must respect copyright and licensing rules when downloading or sharing material.
- USB drives and removable media should be avoided. If used, they must be encrypted where possible and kept secure.

13. Social media and website administration

- Only authorised users may post on or administer council social media accounts or the council website.
- Administrator access must use strong unique passwords and MFA wherever available.
- Passwords for council social media and website accounts must not be held only by one individual.
- Posts and comments must comply with the Members' Code of Conduct, employee standards, equality obligations, data protection rules and any separate council communications or social media policy.
- Personal social media accounts must not give the impression that the user is speaking on behalf of the council unless authorised.

14. Monitoring and audit

The council may review usage logs and records relating to council-owned equipment and council systems where this is necessary and proportionate, for example to maintain security, investigate faults, investigate suspected misuse, comply with legal obligations, recover council records or protect public funds.

The council will not routinely monitor personal use of personal devices. Any access to logs, records or device information must be limited to what is necessary and must comply with data protection and privacy obligations.

15. Security incidents and reporting

Users must report the following to the Clerk as soon as possible, ideally the same day:

- lost or stolen devices that can access council email or documents;
- suspected unauthorised access to a council account;
- phishing emails, suspicious attachments or links that have been opened;
- accidental disclosure of personal data or confidential council information;

- malware infection or suspected compromise of a device used for council business;
- payments, bank details or supplier changes that appear suspicious.

The Clerk, in consultation with the Chair where appropriate, will take reasonable steps to contain the incident, seek advice where needed, reset passwords, disable access, preserve records and consider whether any data protection notification is required.

16. Starters, leavers and role changes

- New users will receive access appropriate to their role and a copy of this policy.
- Access rights should be reviewed when a user changes role.
- When a councillor, employee, contractor or authorised volunteer leaves, the council will remove or disable their council accounts and access rights promptly.
- Leavers must return council-owned equipment and delete local copies of council information from personal devices, personal email and personal cloud storage unless there is a lawful reason to retain them.
- Council records held by a leaver must be transferred to the Clerk or stored in the council's approved system.

17. Review

This policy will be reviewed every two years, or sooner following a significant cyber incident, change of council systems, change in legal requirements, or change in national guidance.

Appendix 1 - BYOD quick checklist

Before using a personal phone, tablet, laptop or desktop for council business, each user should be able to answer Yes to the following:

Control	Requirement
Supported device	My device still receives security updates.
Updates	Automatic updates are enabled where available.
Screen lock	My device has a PIN, password, passphrase, fingerprint or face unlock.
Auto-lock	My device locks automatically after a short period of inactivity.
Separate accounts	Family members or friends cannot access my council email or council documents.
MFA	MFA is enabled on my council accounts wherever available.
Passwords	My council passwords are strong, unique and not shared.
Cloud storage	Council documents are stored in council-approved systems, not personal cloud storage.
Local files	I delete downloaded council files when they are no longer needed locally.
Phishing	I know to report suspicious links, attachments, payment requests and bank detail changes.
Leaving	I understand I must delete council data and return council equipment when my role ends.

Appendix 2 - Security incident quick guide

Scenario	What to do immediately
Lost or stolen device	Tell the Clerk. Change council passwords. Use remote lock/wipe if available. Contact the network provider for a lost mobile phone if needed.
Clicked a suspicious link or opened a suspicious attachment	Disconnect from the internet if malware is suspected. Tell the Clerk. Do not delete evidence. Change passwords from a different trusted device if advised.
Council email account may be compromised	Tell the Clerk. Change the password. Check MFA settings and forwarding rules. Warn relevant contacts if suspicious emails may have been sent.
Accidental email to wrong recipient	Tell the Clerk. Ask the recipient to delete the message if appropriate. Record what was sent, to whom, and when.
Suspicious payment or bank detail change	Do not make the payment until independently verified. Tell the Clerk/RFO and Chair. Use a known phone number, not one in the suspicious message.

Optional user declaration

I confirm that I have read and understood this policy and that any personal device I use for council business meets the BYOD quick checklist, or I will tell the Clerk where it does not.

Name: _____

Role: _____

Signed: _____ Date: _____