MELKSHAM WITHOUT PARISH COUNCIL

IT and Cyber Security Policy:

1. Introduction:

Melksham Without Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors using Melksham Without Parish Council's IT Systems. This is to ensure that council data is protected, security is maintained, and UK legislation and parish council policies are complied with.

The parish council's IT contractor is Clive Merritt from Avon IT.

2. Scope

This policy applies to all parish councillors, employees, volunteers, and contractors who use Melksham Without Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Melksham Without Parish Council IT resources and email accounts are to be used for official council related activities and tasks. All members will be provided with a council e-mail address and must use this for all council business. No parish council communications should be undertaken using personal email accounts. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device Security and software usage

Where possible, authorised devices, software, and applications will be provided by Melksham Without Parish Council for work-related tasks. Devices and equipment provided by the council remain the property of Melksham Without Parish Council and are recorded in the asset register. Unauthorised installation of software on parish council devices, including personal software, is strictly prohibited due to

security concerns. Upon leaving office or employment, users must return all Council-issued equipment immediately to the Clerk.

System Updates:

System updates provide essential security fixes to protect against cyber threats, deliver performance enhancements and bug fixes to improve system stability and speed. In order for system updates to be undertaken, all users must regularly switch off their laptops.

Anti-Virus:

All Council devices must have up-to-date anti-virus and anti-malware software installed, this can be in the form of the following:

- Non-Finance Committee Councillors: Free version of Avast is sufficient as members are only accessing office 365 and the device has no access to the council's networks,
- Finance Committee members: A business grade anti-virus should be installed on these members laptops due to them being used occasionally to undertake online bank authorising.
- For the three officer laptops, server computer and meeting room device, the business grade anti-virus should be installed due to them all having access to the councils shared drive and network.

All parish council laptops have a built in Windows Firewall and Staff, councillors, and volunteers must not disable or uninstall anti-virus software without prior authorisation from the parish council.

Any suspected virus or malware infection must be reported immediately to the Clerk so that swift action can be taken.

5. Data management and security

All sensitive and confidential Melksham Without Parish Council data should be stored and transmitted securely using approved methods. Data is backed up in the Microsoft 365 cloud; however regular data backups from the server computer should be performed to prevent data loss and protect council records in the instance where the cloud data gets corrupted. Secure data destruction methods should be used when necessary. All users must comply with the council's Data Protection & Retention Policy.

6. Network and internet usage

Melksham Without Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Melksham Without Parish Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is marked as such. All users should be cautious with attachments and links to avoid phishing and malware if unsure about their legitimacy the source should be verified before opening any attachments or clicking on links. Users should never share passwords via email and should be cautious of odd or inconsistent language in communications. Emails relating to council business are considered council data and may be subject to disclosure under the Data Protection Act or Freedom of Information Act.

8. Password and account security

Melksham Without Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others and where available/ accessible, Two-Factor Authentication should be used. The parish council shared drive holds a password protected list of passwords for officers to access in order to undertake parish council work. These passwords are for accounts where more than one officer needs to access the account. Passwords relating to email accounts and council bank accounts are not included on this list. Access to systems is limited to those who need it for their role. For some websites and accounts officers save the password to the laptop or personal mobile as they access very regularly (eg facebook account, email) but do not do for other accounts and never for anything financial eg banking, or the council debit card details.

Password Management System:
Staff are able to use an approved password management system for storing and accessing passwords relating to parish council business. All council related passwords should be kept within the password management system and once implemented must not be stored or shared by other methods.

When a councillor or staff member leaves, their online access to their emails and office 365 account is immediately revoked. In the event that a councillor resigns during their term of office, their council email inbox will be temporarily redirected to the Clerk to ensure continuity of communication and to receive any council related correspondence from residents. This arrangement will remain in place until a new councillor is formally appointed. Upon the appointment of a new councillor, the former councillor's email account will be permanently closed and all data, including emails, will be deleted.

When a council employee leaves their position, their email account will be retained and reassigned to their successor to ensure continuity of service and access to relevant historical correspondence.

The Clerk and IT contractor have administrator access to the council's office 365 accounts.

Regular password changes are encouraged to enhance security.

9. Mobile devices and remote Work

Mobile devices provided by Melksham Without Parish Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office. Parish Council systems (including email, websites and data) can be accessed via personal devices, but they must be password protected, and access is restricted solely to that member or employee. No items should be downloaded onto the device.

10. Social Media:

Council social media accounts will be operated by officers.

The parish council have a separate social media policy in place, please refer to this for guidance.

11. Email monitoring

Melksham Without Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

Refer to the email policy

12. Parish Council Website:

The Council website is hosted under the .gov.uk domain and is maintained by council officers with support from the council's IT contractor. For the current website, only the three officers (Clerk, Finance & Amenities Officer and Parish Officer) and the council's IT contractor have admin access to the content management system. The officers as specified above are responsible for updating, uploading and managing the website content in accordance with council procedures and statutory requirements. No councillor or other external party has admin access to the websites content management system.

All users as specified above who have access to the content management system must adhere to this IT policy.

13. Melksham Neighbourhood Plan website:

The parish council jointly manage the Melksham Neighbourhood Plan website with Melksham Town Council. The website was created by Place Studio and is hosted by WIX. The admin area of the website can be access by officers of both councils

who are able to update and add content as well as Place Studio under the direction of the Neighbourhood Plan Steering Group/ both councils.

14. Use of WhatsApp Communications:

WhatsApp may be used by council staff for informal and operational communication relating to council business. Its purpose is to support day to day operation, when staff are either working remotely or responding to issues in the parish.

Typical uses of WhatsApp include:

- Monitoring and reporting on grounds maintenance, street furniture, and other public amenities (allotments and sports field).
- Sharing images/ videos of council events, assets and projects
- Communicating with contractors where appropriate. (This does not replace the use of email and any official order for works is always sent by council email to the contractor's official email address.)
- Communicating with Flood Wardens, including during a weather emergency
- Facilitating the Melksham Community Group forum

Staff WhatsApp Groups:

There are two staff WhatsApp groups that have been set up and are currently in use by staff:

Officers: This is for the three council officers and is to facilitate quick, informal communication between officers, in particular when officers are working away from the office.

Staff: This includes the three council officers as well as the two members of the grounds team and is used to facilitate communication relating to the parish amenities in the parish.

This is where the grounds team report any issues to officers and send any related photos through to them. It is also where officers instruct any additional tasks that may be required.

The Finance & Amenities Officer communicates with the Allotment Warden in a private separate WhatsApp Group when matters involved individual allotment holders, plot specific issues or contact details. This is to prevent unnecessary sharing of personal data.

Important Notes on WhatsApp Use:

- Official council business should be conducted through formal channels such as council email or meeting.
- All WhatsApp groups established by the Parish Council must comply with GDPR 2018.

- Formal decisions cannot be made via WhatsApp and must be ratified through the proper channels.

15. Use of Shared Drives with external parties:

Shared drives may be used to facilitate secure file sharing with external parties, such as contractors, consultants, other councils and volunteers. Access will be granted solely to support the delivery of the agreed parish council project/activity. Access will only be provided on the basis of what is necessary to share and will be limited to the minimum folders and files required in order for the external party to carry out their role. All external parties will be approved by the Clerk before being given access to the folders/files.

Any files or folders provided in the shared drive must be used only for the purpose for which it has been provided, and all external parties must comply with the council's policies around GDPR.

Avon IT, as the parish councils IT contractor has admin access to the parish council's office 365 accounts and as such, has access to all of the councils shared drive documents in order to undertake his role for the parish council.

All external parties will be asked to read and sign the parish councils Data Processing agreement before being given access to any of the parish councils documents.

16. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

Refer to the policy just reviewed at Full Council November 25 – Retention and Disposal Policy

17. Incident Reporting

All suspected security breaches or incidents should be reported immediately to the Clerk for investigation and resolution. All users should report any email-related security incidents or breaches to the Clerk immediately. This includes:

- Potential risk arising from phishing emails/websites
- Passwords having been shared
- Unauthorised access to system

Users must report lost, stolen, or damaged equipment immediately to the Clerk. If criminal activity is suspected, the Clerk will report the incident to the Police. The Clerk will (Or instruct Avon IT) to change the password to the member or employee's office 365 account.

18. Training and awareness

Melksham Without Parish Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

19. Compliance and consequences

Breach of this IT and Email Policy and misuse of IT systems may result in the suspension of IT privileges and further consequences as deemed appropriate. Misuse includes but is not limited to:

- Accessing, creating or sending offensive or inappropriate content
- Sending defamatory or infringing material
- Distributing spam or malware
- Interfering with others' data or work
- Changing system settings without permission
- Using council devices for gaming during work-related activities
- Unauthorised access to or distribution of council systems, data or information is strictly prohibited.

20. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

21. Contacts

For IT-related enquiries or assistance, users can contact the Clerk. All staff and councillors are responsible for the safety and security of Melksham Without Parish Council's IT and email systems. By adhering to this IT and Email Policy, Melksham Without Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

Adopted by Parish Council 8th December 2025

Version table:

Version	Meeting date and meeting	Amendment/ changes made
1.0	Reviewed and recommended at IT Working Party 28th November 2025 and adopted by Council at Full Council 8th December 2025 (min.360/25b)	Adoption of IT and Cyber Security Policy