Morwenstow Parish Council

IT Policy

Morwenstow Parish Council (Known throughout this policy as MPC) understands and acknowledges the importance of effective and secure information technology (IT) and email used in supporting its business, operations, and communications.

Purpose

The purpose of this policy is to ensure the secure, effective, and lawful use of IT systems, devices, and data by employees, councillors, volunteers, and contractors of MPC. It aims to protect the council's IT assets, uphold data protection principles, and promote responsible IT usage.

MPC is committed to ensuring that all IT resources are used responsibly, securely, and effectively, by setting out the standards for the use of MPC-owned IT equipment, software, and internet access by MPC members, employees, and volunteers. It also outlines recommendations on use of social media both professionally and personally (due to the potential for impact on MPC).

Scope

This policy applies to all individuals who use MPC IT resources, including computers, laptops, networks, software, devices, and data – whether MPC owned or on personal devices. Such resources include access to .gov.uk email addresses and any associated digital storage.

Acceptable Use

All users must:

- Use IT equipment and services provided by MPC for council-related work only, and in accordance with all aspects of this policy.
- Use only MPC email addresses (.gov.uk) for official correspondence, and all MPC related work.
- Ensure sensitive or confidential data is handled appropriately and securely.
- Report suspected data breaches, malware, or IT issues directly to the clerk at Clerk@morwenstowparish.gov.uk and not through a third party.
- All users must adhere to ethical standards, respect copyright, and intellectual property rights, and avoid accessing inappropriate or offensive content.

Device and software usage

Authorised devices, software, and applications are provided by MPC to the Clerk/RFO for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

Unacceptable Use

The following are strictly prohibited:

- Using MPC IT systems for personal gain, illegal activities, or political campaigning.
- Accessing, storing, or sharing offensive, abusive, or inappropriate content.
- Installing unauthorised software or altering system settings.
- Using MPC devices to conduct private business or unrelated activities.
- Connecting unapproved personal devices to MPC networks without prior consent from MPC.

Data Protection and Confidentiality

All users must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This includes:

- Keeping personal data secure and confidential.
- Not disclosing information without proper authorisation.
- Using encryption and secure storage where required.

Data Management and Security

All sensitive and confidential MPC data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

Any suspected security breaches or incidents should be reported immediately to the Clerk, who is MPC's designated IT point of contact for investigation and resolution.

Email and Internet Use

- MPC email must be used professionally and responsibly AT ALL TIMES.
- Emails sent on behalf of MPC must be relevant to MPC matters.
- Emails should be professional and respectful in tone.
- Internet usage on MPC owned equipment should be appropriate and in line with MPC policies and responsibilities.
- Any confidential or sensitive information must *not* be sent via email unless it is encrypted.
- Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

- Users must not download unauthorised software or access inappropriate websites.
- Emails should be retained and archived in accordance with legal and regulatory requirements, with regular reviews and deletion of unnecessary emails to maintain an organised inbox.

Security and Updates

- Users must not disable or bypass antivirus or security settings.
- MPC devices must be kept up to date with security patches and software updates.
- Lost or stolen devices must be reported immediately.

Remote Working

When working remotely the preference is to use only MPC-approved devices. If it does become necessary to use personal devices for conducting ANY MPC business, users are required to,

- Ensure the personal device meets all security standards of MPC devices.
- Avoid using public Wi-Fi without a secure connection (e.g. VPN).
- Maintain confidentiality, especially in shared or public spaces.

Any work done on user's own equipment should be stored securely and password protected and should always be backed up in accordance with MPC's standard backup procedures.

All Mobile/Portable devices provided by MPC should be secured with passcodes and/or biometric authentication. All users should follow the same security practices as if they were based in an office. This applies to all MPC provided and personal devices used for MPC work. Failure to comply may lead to disciplinary action.

All computer and other electronic equipment supplied must be treated with good care at all times.

Computer and electronic hardware must be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on MPC.

Equipment must not be dismantled or reassembled without seeking advice.

Councillors, staff, and other authorised are not to purchase any computer or mobile equipment (including software), unless previously agreed and authorised by MPC.

Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on MPC computers without the prior approval of the Clerk.

Portable Equipment

All portable computers must be stored safely and securely when not in use, i.e. when travelling or when working from home. Portable equipment (unless locked in a secure cabinet or office) must be

kept with or near the user at all times; must not be left unattended when away from the usual workplace and must never be left in parked vehicles at any time.

It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold MPC data, including emails and files, must be protected with a pin code. Where possible, these devices must also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disenabled or removed.

Multi-Factor Authentication (MFA) is a security process that requires users to verify their identity using two or more independent methods—for example, entering a password (something you know) and confirming a code sent to your mobile device (something you have). This significantly reduces the risk of unauthorised access to systems and sensitive data. NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018.

If an item of portable equipment is lost or damaged this must be reported to the clerk, and/or the Chair. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet part of the cost of the loss/damage.

Password and Account Security

MPC IT users are responsible for maintaining the security of their accounts and passwords. Passwords must be strong and not shared with others. Regular password changes are encouraged to enhance security.

All user accounts must be protected by strong, secure passwords. The National Cyber Security Centre (NCSC) recommends creating passwords using three random words (e.g. PurpleCandleRiver). This method helps create passwords that are both strong and easy to remember, while offering effective protection against common cyber threats such as brute-force attacks. This approach is endorsed in NALC guidance.

Use of social media

Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); virtual worlds (Second Life); text messaging and mobile device communications and more traditional forms of media such as TV and newspapers.

Care must be taken when using social media at any time, either using MPC systems or at home. MPC recognises the importance of social media in helping to shape sector conversation and enhancing its image through interaction on social media. Therefore, where it is relevant to use social networking sites as part of MPC position, this is acceptable. However, inappropriate comments and postings can adversely affect the reputation of MPC, even if it is not directly referenced. Therefore, even on personal social media accounts, councillors, the clerk, and other stakeholders must take care when responding to other users.

If comments or photographs could reasonably be interpreted as being associated with MPC, or if remarks about could be regarded as abusive, humiliating, threatening, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, MPC will treat this as a serious disciplinary offence.

Councillors, staff, and other authorised users must be aware that parishioners or other local organisations may read councillors, staff, and other authorised users' personal social media, to acquire information, for example, about their work, internal MPC business, and employee morale. Therefore, even if MPC is not named, care must be taken with any views expressed.

To protect both MPC and its interests, everyone is required to comply with the following rules about social media, whether in relation to their MPC role or personal social networking sites, and irrespective of whether this is during or after working hours:

Contacts from any MPC databases must not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.

Any social media post that mentions MPC, its current work, councillors, employees, other users associated with MPC, partner organisations, local groups, suppliers, parishioners, must identify the author as one of its councillors or employees and state that the views expressed are theirs alone and do not represent the views of MPC.

Comments posted by councillors, staff, and other authorised users on any social media or websites must be knowledgeable, accurate and professional and must not compromise MPC in any way. Therefore, writers must not claim or give the impression that they are speaking on behalf of MPC – unless authorised to do so. Even if MPC is not mentioned, care must be taken with any personal views expressed on social media sites and within such views it must be clearly stated these are the writer's own (e.g. via a disclaimer statement such as: "*The comments and other content on this site are my own and do not represent the positions or opinions of MPC."*

MPC expects councillors, staff, and other authorised users to be respectful about MPC and its current or potential work and not engage in any name calling, nor in any behaviour that will reflect negatively on the reputation of MPC – such as making threats, harassment, or bullying.

Any unauthorised use of copyright materials, any unfounded or derogatory statements, or any misrepresentation not viewed favourably, could constitute gross misconduct.

Any writing about, or displaying photos or videos of any internal activities involving current councillors, staff, and other authorised persons, might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, their permission must be gained from all individuals concerned - prior to uploading any such material.

Details of any kind relating to any events, conversations, materials, or documents that are meant to be private, confidential, or internal to MPC must not be posted. This may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other councillors, staff, and other authorised users anything to do with a disciplinary case, grievance, allegation of bullying/harassment or discrimination, or legal issue; any other secret, confidential, or proprietary information or information that is subject to confidentiality agreements. This does not affect statutory requirements to publish information including under the Freedom of Information Act.

Councillors, staff, and other authorised users must be aware that they are personally liable for anything that they write or present online (including on online forum, blog, post, feed, or websites).

Councillors must always be mindful of the Members Code of Conduct and Nolan Principles AT ALL TIMES.

Councillors and Employees may be subject to disciplinary action for comments, content, or images that are defamatory, embarrassing, pornographic, proprietary, harassing, libellous, or that can create a hostile work environment. They may also be sued by other organisations, and any individual or council that views their comments, content, or images as defamatory, pornographic, proprietary, harassing, libellous or creating a hostile work environment. In addition, other councillors, staff, and other authorised users can raise grievances for alleged bullying and/or harassment.

Contacts by the media relating to MPC and/or to any work MPC may be involved with, must always be referred to the clerk.

Councillors, staff, and other authorised users who use sites such as LinkedIn and Facebook must ensure that the information on their profile is accurate and up to date and they must update their profile on leaving MPC.

Councillors, staff, and other authorised users who have left MPC must not post any inappropriate comments about MPC or its councillors, staff, and other authorised users on LinkedIn, Facebook, X.com or any other social media/networking sites.

During any employment and/or involvement with MPC, you may create or obtain access to a variety of professional contacts and confidential information. This includes, but is not limited to, contacts made through professional networking platforms such as LinkedIn, where those contacts have been established or maintained in your capacity as a councillor, member of staff, or any other authorised user. All such contacts will be considered MPC property and may be subject to disclosure upon request.

Note that MPC may, from time to time, monitor external postings on social media sites. Any councillor or employee who has a profile (for example on LinkedIn or Facebook) must not misrepresent themselves or their role with MPC. Councillors, staff, and other authorised users are also advised that social media sites are not an appropriate place to air MPC concerns or complaints: these must be raised with MPC or formally through the grievance procedure.

Disposal of Equipment

Prior to the disposal of any device that may contain, store, or hold data related to MPC and its work, and/or in the event of a user leaving MPC, councillors, staff, and other authorised users are required to allow the Clerk access to the device to ensure that all passwords, user access shortcuts. and any identifiable data are removed from the device.

Monitoring and Compliance

As an IT provider, MPC has the right to monitor the use of its IT equipment and any systems. MPC 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.

Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use MPC systems e.g. if they have a council e-mail address.

Compliance and Consequences

Breaches of this policy may result in disciplinary action or withdrawal of IT privileges. Serious breaches may be reported to the Information Commissioner's Office (ICO) or law enforcement.

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.

All staff and councillors are responsible for the safety and security of MPC's IT and email systems. By adhering to this IT and Email Policy, MPC aims to create a secure and efficient IT environment that supports its mission and goals. As such this Document must be read in Conjunction with the following MPC Policies

a) *General privacy Notice*
b) *Data protection Policy*
c) Website Privacy and terms of use Policy
d) Community Centre Wi-Fi Policy

Policy formally adopted by Morwenstow Parish Council on - 21st January 2026

Signed by Chair Proposed by Cllr. Jonathan Hobbs. Seconded Cllr Myers

Minute reference 21.01.2020.10.1d

Date of Review	Reviewed by	Minute Reference
January 2027		