MARDEN PARISH COUNCIL
INFORMATION TECHNOLOGY POLICY

1. Introduction

Marden Parish Council (MPC) has its own small IT infrastructure and has created this IT policy based on NALC guidelines. These guidelines are intended to help councils identify key considerations when developing or updating their own IT policy. This policy reflects the guidelines and takes into account the service providers and operational requirements and needs of staff and councillors.

"The Clerk" also means the Deputy Clerk in the Clerk's absence.

2. Purpose of the IT Policy

The purpose of this policy is to establish and communicate clear parameters for how councillors, staff and other authorised users use council provided technology or equipment and IT resources in the course of their duties. This therefore applies to all individuals who use MPC's IT resources, including computers, networks, software, devices, data and email accounts.

This Policy is intended to:
- Set expectations for appropriate use of equipment and systems.
- Raise awareness of risks associated with IT use.
- Safeguard the council's data and digital assets.
- Clarify what constitutes acceptable and unacceptable use.
- Outline the consequences of policy breaches.
- Provide guidance on the personal use of MPC computers/equipment.
- Outline email usage for staff and councillors.

This policy will also state what constitutes personal use of IT equipment and what is/is not permitted. Only those persons authorised by the Parish Clerk are permitted to post material, or use the MPC's logo, heading or imagery on social media and websites in MPC's name and on its behalf.

3. Monitoring of IT Use

As an IT provider, MPC has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors, employees and other authorised users are informed that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws. Other persons may be included if they access or use council systems e.g. if they have a council e-mail address.

4. Scope of this policy

This policy applies to all councillors, staff, and other authorised users, regardless of their working location or pattern, including those who are home-based, office-based, or work on a flexible or part-time basis. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

5. Computer use
Hardware
(1)	Council computer equipment is provided for council purposes; however reasonable, short duration personal use is permitted (reasonable interpreted as in the opinion of MPC and the Clerk). Any personal use of MPC's computers and

systems should not interrupt the daily council work in any way. Staff and other authorised users are asked to restrict any personal use to official lunchbreaks, or outside working hours.

(2)   Locking computers to sleep mode or turn off completely when leaving desk to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

(3)   All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.

(4)   Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

(5)   Equipment should not be dismantled or reassembled without seeking advice.

(6)   Councillors, staff, and other authorised are not to purchase any computer or mobile equipment (including software). Unless previously authorised.

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

(8)   A portable device to make personal Wi-Fi hot spots is only permitted when equipment is used off site when Wi-Fi is not available.

(9)   Any faults or necessary repairs must be reported to the Clerk in the first instance and then CloudyIT (MPC's IT provider) if problem persists.

6. Equipment
Portable equipment
(1)   Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

(2)   It is particularly emphasised that council back-up procedures specific to portable equipment should be followed at all times.

(3)   When possible, all portable computers must be stored safely and securely when not in use in the office, i.e. when travelling or when working from home. Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left in parked vehicles or at any council or non-council premises.

(4)   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. MFA must be used when accessing confidential and financial data on 3rd party systems.

(5)   If an item of portable equipment is lost or damaged this should be reported to the Clerk/MPC Chairman. All users must take the appropriate steps to ensure the safety and integrity of equipment.

(6)   To protect confidential information, unless it is a requirement of the job and this has been authorised, it is forbidden for photographs or videos to be taken on council premises, without the prior permission of the Clerk/MPC Chairman. This includes mobile telephones with camera function, camcorder, tape or other recording device for sound or pictures - moving or still.

(7)   Under no circumstances should any non-public meeting or conversation be recorded without the permission of those present. This does not affect statutory rights (under The Openness of Local Government Regulations 2014).

(8)   In addition, the council does not permit webcams (which may be pre-installed on many laptops) to be used in the workplace, other than for conference calls for council purposes. If there is any doubt as to whether a device falls under this clause, advice should be sought from the Clerk.

Use of own devices
(9)   The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access a limited number of Internet Cloud Based services such as Email. Access to confidential data on 3rd party networks via the office internet should comply with MFA. Access to MPC network is restricted by password and access will be granted by the Clerk.

(10)   Personal devices will not be permitted to access MPC confidential servers and given access to services such as our servers, private clouds or networks for normal council purposes including accessing documents stored on MPC's network or to store data on the council's server(s) or access data in other services.
Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) will normally be permitted. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

(11)   However, the same security precautions apply to personal devices as to MPC's desktop equipment. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

(12)   Councillors, staff, and other authorised persons that use council systems are expected to use all devices in an ethical and respectful manner and in accordance with this policy. Accessing inappropriate websites or services on any device via the IT infrastructure that is paid for or provided by the council carries a high degree of risk, and, for employees, may result in disciplinary action, including summary dismissal (without notice). For Workers or Contractors, MPC may terminate the worker agreement. This is irrespective of the ownership of the device used. An

example would be downloading copyright music illegally or accessing pornographic material.

(13)   In cases of legal proceedings against the council, the council may need to temporarily take possession of a device, whether council-owned or personal to retrieve the relevant data.

(14)   Wherever possible the user should maintain a clear separation between the personal data processed on the council's behalf and that processed for their own personal use, for example, by using different apps for council and personal use. If the device supports both work and personal profiles, the work profile must always be used for work-related purposes.

15)   Councillors, staff, and other authorised users who intend to use their own devices via the council's infrastructure must ensure that they:

- use a strong password or fingerprint/face recognition to protect their device(s) from being accessed. For smartphones and tablets this should lock the device after 5 failed login attempts.
- configure their device(s) to automatically prompt for a password after a period of inactivity of more than 15 minutes.
- always password protect any documents containing confidential information that are sent as attachments to an email, and notify the password separately (preferably by a means other than email).
- Councillors, staff, and other authorised users are advised to keep personal data separate from council data where possible.
- ensure secure Wi-Fi networks are used.
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device.
- inform the Clerk/MPC Chairman if their device(s) is/are lost, stolen, or inappropriately accessed where there is risk of access to council data or resources. To prevent phones being used, it is recommended to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

(16)   Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

(17)   If removable media are used to transfer data (e.g. USB drives or CDs), the user must also securely delete the data on the media once the transfer is complete.

(18)   Councillors, staff, and other authorised users who open any attachments should ensure that any cached copies are deleted immediately after use. The Clerk/CloudyIT will provide assistance or training in doing this if needed. Additional risks include data belonging to the council being accessed by unauthorised persons if the device(s) is lost, stolen, or used without the owner's permission.

(19)   Councillors, staff, and other authorised users must take responsibility for understanding how their device(s) work in respect to the above rules if they are

accessing council services via their own IT equipment. Risks to the user's personal device(s) include data loss as a result of a crash of the operating system, bugs and viruses, software or hardware failures and programming errors rendering a device inoperable. The council will use reasonable endeavours to assist, but councillors, staff, and other authorised users are personally liable for their own device(s) and for any costs incurred as a result of the above.

7. Health and Safety

(1)   Councillors, staff, and other authorised users who work in council offices will be provided with an appropriate workstation.

(2)   The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment. Further details are set out in MPC's health and safety policy.

(3)   Any VDU user who feels that their workstation requires changes to make it compliant must speak to the Clerk/HR Committee.

(4)   If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the Clerk/CloudyIT.

8. Password and Authentication Policy

(1)   All user accounts must be protected by strong, secure passwords. It is recommended that when creating passwords three random words (e.g. PurpleCandleRiver) are used. 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.

(2)   In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA requires users to provide two or more independent forms of verification—for example, a password (something you know) and a code sent to your phone (something you have). This significantly reduces the risk of unauthorised access to systems and personal data.

(3)   To further strengthen account security:
- Initial user account passwords must be generated by the IT provider.
- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- Service or System (e.g. Website) account passwords are generated and managed by the IT provider.
- The council recommends these practices as part of its commitment to robust information security and to support compliance with the UK GDPR and the Data Protection Act 2018.

For more guidance, see the NCSC's advice on password security: NCSC Password Guidance

Access to Passwords

(5)   Passwords are personal and must not be shared under any circumstances.

(6)   Only the assigned user of an account may access or use the associated password.

(7)   In exceptional cases (e.g., incident response or employee offboarding), access to system credentials may be granted to authorised personnel from the IT provider with appropriate approvals and logging.

(8)   Administrative credentials must be stored securely and only accessible to authorised personnel with a copy made available to MPC Chairman (stored in the office fire safe in a sealed envelope and only to be accessed in an emergency).

Password Storage and Management
(9)   Passwords must not be stored in plain text or written down in insecure locations.

Password Change Requirements
(10)   Immediately change password if compromise is suspected.

Password Access Control and Logging
(11)   All access to administrative or shared credentials must be logged and auditable.

(12)   Attempts to access unauthorized passwords will be treated as a security incident.

Responsibility
(13)   Users are responsible for creating and maintaining secure passwords for their accounts.

(14)   IT security provider is responsible for:
- Managing system/service credentials.
- Enforcing password policies. Auditing and monitoring password-related security practices).

9. Monitoring
(1)   MPC reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

(2)   MPC may monitor the use of electronic communications and use of the internet in line with the Investigatory Powers (Interception by Councils etc for Monitoring and Record-keeping Purposes) Regulations 2018.

(3)   MPC reserves the right to monitor an employee's email and/or internet use in accordance with an impact assessment that MPC has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in MPC's legitimate interests and is to ensure that this policy is being complied with.

(4)	The information obtained through monitoring may be shared internally, including with relevant councillors and IT staff if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

(5)	The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

(6)	Councillors, staff, and other authorised users have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in MPC's Data Protection Policy.

(7)	Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

(8)	MPC reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. MPC also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

(9)	Any use by staff that MPC considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

(10)	All computers will be periodically checked and scanned for unauthorised programmes and viruses.

## 10.	Remote working
(1)	Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling, working from home or at any other different venue), as follows:

- if logging into MPC's systems or services remotely, using computers that either do not belong to MPC or are not owned by the user, any passwords must not be saved, and the user must log out at the end of the session deleting all logs and history records within the browser used. If the configuration of the devise does not clearly support these actions (for example at an internet café), council services should not be accessed from that device.
- the location and direction of the screen should be checked to ensure confidential information is out of view. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc.
- any data printed should be collected and stored securely.
- all electronic files should be password protected and the data saved to the council's system/services when accessible.

- papers, files or computer equipment must not be left unattended at non-council premises unless arrangements have been made with a responsible person at a non-council premises for them to be kept in a locked room or cabinet if they are to be left unattended at any time.
- any data should be kept safely and should only be disposed of securely.
- papers, files, data sticks/storage, flash drive or backup hard drives should not be left unattended in cars, except where it is entirely unavoidable for short periods, in which case they must be locked in the boot of the car. If staying away overnight, council data should be taken into the accommodation, care being taken that it will not be interfered with by others or inadvertently destroyed.
- where possible the ability to remotely wipe any mobile devices that process sensitive information should be retained in the case of loss or theft.
- Councillors, staff, and other authorised users who work away from the office with sensitive data should be equipped with a screen privacy filter for mobile devices and should use this at all times when accessing such data away from the office.

11. Email

(1)   Council email facilities are intended to promote effective and speedy communication on work-related matters. Although MPC encourages the use of email, it can be risky. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

(2)   On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors, staff, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

(3)   These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask CloudyIT, rather than assuming they know the right answer.

(4)   All Councillors and office staff have a "mardenkent-pc.gov.uk" email account and this email account MUST be used at all times for Council business only. Personal emails should NOT be used for Council work nor linked to Council email accounts. MPC may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

(5)   Emails designated as a record (a record is any document, file, email or other form of information regarded as evidence of business activities, decisions, transactions or communications etc) should be retained and archived in accordance with legal and regulatory requirements. Regular reviews and deletion of unnecessary emails should be undertaken in line with GDPR/DPA and to maintain an organised mailbox.

(6)   Cllrs and staff should be aware that they must never forward information of a confidential nature to outside parties.

12. Use of the Internet
Copyright
(1)   Much of what appears on the Internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited. The Copyright, Designs and Patents Act 1988 set out the rules. The copyright laws not only apply to documents but also to software. The infringement of the copyright of another person or organisation could lead to legal action being taken against the council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

(2)   It is easy to copy electronically, but this does not make it any less an offence. MPC's policy is to comply with copyright laws, and not to bend the rules in any way.

(3)   Councillors, staff, and other authorised users should not assume that because a document or file is on the Internet, it can be freely copied. There is a difference between information in the 'public domain' (which is no longer confidential or secret information but is still copyright protected) and information which is not protected by copyright (such as where the author has been dead for more than 70 years).

(4)   Usually, a website will contain copyright conditions; these warnings should be read before downloading or copying.

(5)   Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the Clerk or CloudyIT if unsure about anything.

Trademarks, links and data protection
(6)   MPC does not permit the registration of any new domain names or trademarks relating to MPC's names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of MPC's web pages to any other external sites without checking first with Clerk/MPC.

(7)   Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's Data Protection Policy, a copy of which is available from the Clerk and on MPC's website.

Accuracy of information
(8)   One of the main benefits of the internet is the access it gives to large amounts of information, which is often more up to date than traditional sources such as libraries. Be aware that, as the internet is uncontrolled, much of the information may be less accurate than it appears.

13.   Use of social media

(1)   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 should be taken when using social media at any time, either using council systems or at home.

(2)   Personal use of social networking/media and chat sites should be restricted to breaks during working hours.

(3)   MPC recognises the importance of councillors, staff, and other authorised users joining in and helping to shape sector conversation and enhancing its image through blogging and interaction in social media. Therefore, where it is relevant to use social networking sites as part of the individual's position, this is acceptable.

(4)   However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be interpreted as being associated with MPC, or if remarks about others could be regarded as abusive, humiliating, 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 should be aware that parishioners or other local organisations may read councillors, staff, and other authorised users' personal weblogs, to acquire information, for example, about their work, internal council business, and employee morale. Therefore, even if MPC is not named, care should be taken with any views expressed.

(5)   To protect both MPC and its interests, everyone is required to comply with the following rules about social media, whether in relation to their council role or personal social networking sites, and irrespective of whether this is during or after working hours:
- MPC will treat everyone with courtesy and respect on its social media channels and therefore request for the same in return from those who choose to engage with MPC.
- Contacts from any of MPC's databases should not be downloaded and connected with on LinkedIn or other social networking sites with electronic address book facilities, unless this has been authorised.
- Any blog that mentions MPC, its current work, councillors, employees, other users associated with MPC, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or employees and state that the views expressed on the blog or website are theirs alone and do not represent the views of MPC. Even if MPC is not mentioned, care should be taken with any views expressed on social media sites and any views should clearly be stated to be 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 my employer/ MPC.") Writers must not claim or give the impression that they are speaking on behalf of MPC.
- Any employee who is developing a site or writing a blog that will mention MPC, [e.g. "our current or potential plans, councillors, staff, and other authorised users, partners"], must inform the Council that they are writing this and gain agreement before going 'live'.
- The council expects councillors, staff, and other authorised users to be respectful about MPC and its current or potential staff, including employees, councillors, clerks, and authorised users and not to engage in any name calling or any

behaviour that will reflect negatively on its reputation. Any unauthorised use of copyright materials, any unfounded or derogatory statements, or any misrepresentation is not viewed favourably and could constitute gross misconduct.

- Photos or videos that include employees or other workers wearing uniforms or clothing displaying MPC's name or logo should not be posted on social media if they could reflect negatively on the individual, their role, their colleagues, or MPC. Additionally, photos, videos, or audio recordings must not be taken on council premises without explicit permission

- Comments posted by councillors, staff, and other authorised users on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.

- Inappropriate conversations with anyone should not take place on any social networking sites, including forums.

- Any writing about or displaying photos or videos of internal activities that involves 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 should be gained 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 the council should 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 an online forum or blog, post, feed or website). Councillors should always be mindful of the Members Code of Conduct and Nolan Principles of conduct in public life (*The 7 Principles of Public Life: Selflessness; Integrity; Objectivity; Accountability; Openness; Honesty and Leadership ([The Seven Principles of Public Life - GOV.UK](https://www.gov.uk))*). 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.

- Postings to websites or anywhere on the internet and social media of any kind, or in any press or media of any kind, should not breach copyright or other law or disclose confidential information, defame or make derogatory comments about MPC or its councillors, staff, and other authorised users, or disclose personal data or information about any individual that could breach data protection legislation.

- Contacts by the media relating to MPC, should 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 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 your employment/ 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 other authorised user. All such contacts will be considered council property and may be subject to disclosure upon request.
- Comments should not advertise commercial products or services.

(6)   By choosing to comment and/or utilise any MPC social media sites, users are deemed to agree to this policy.

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

(8)   It is important to note that contact details and information remain the property of the council. In addition, councillors, staff, and other authorised users leaving the council will be required to delete all council-related data including contact details from any personal device/equipment.

14.   **Use of MPC Website**
(1)   MPC is committed to adhering to the Local Government Transparency Code 2015 and providing and promoting access to news, history and information relevant to the Parish of Marden for public access and one of the ways is to maintain a website.

(2)   MPC office staff maintain the website content to ensure it is up to date. All correspondence to MPC via the website will be acknowledged within five working dates of receipt by the Clerk.

(3)   The Clerk and Deputy Clerk will evaluate all potential content requests from outside bodies to ensure it is appropriate for MPC's website.

(4)   The photo gallery is used to store and display photographs of interest appropriate to Marden and is editable by all office staff. Photographs of children can be used on the website without consent only where individuals cannot be identified (eg from a distance). MPC will obtain consent of parent/carer of children if identifiable photos are used. Personal details of children will never be shown in photographs or included in any accompanying text. Photographs showing adults in

group situations or where individuals are unidentifiable are used without seeking consent from those individuals involved. They will be removed upon request by an individual involved.

(5)   MPC's website contains hyperlinks to other public and private organisations websites. External links are identified in the link text or an accompanying description. To be included websites must meet the following criteria:

- The primary intent of the website is to educate or inform.
- The site's owner or sponsor is easily identifiable, and contact information is provided.
- The site does not charge for access.
- The site does not promote a specific political or social agenda.
- The site provides useful information on local services for the community.
- Only Marden, surrounding parishes and local & central government website links will be published.

(6)   Since website content may change or disappear entirely without notice, MPC cannot be held responsible for the content or accuracy of external websites.

15.   Use of WhatsApp

(1)   MPC has agreed that it would be advantageous for MPC Cllrs and employees to have access to WhatsApp messaging groups for the sharing of information outside of formal Council meetings.

(2)   Membership of these groups is discretionary and does not replace the decision-making framework of properly convened meetings and MPC's scheme of delegation.

(3)   These groups will only be for Cllrs and employees of MPC. Any members of the public who are on any of the Sub-Committees/Sub-Groups will be contacted separately via text/email from an Officer to provide the information given in the WhatsApp conversation.

(4)   Mobile phone numbers of MPC Cllrs and employees will be visible to everyone in the group.

(5)   MPC Cllrs and employees who have given their consent for their data to be processed in this way will be added to WhatsApp groups as appropriate.

(6)   A general group may be set up and all Cllrs and employees, who have given their consent, will be members of this group. Additional groups can be set up for individual Sub-Committees/Sub-Groups if appropriate.

(7)   It is for the sharing of information only, for example issuing reminders about meetings, reminders to authorise bank payments, to arrange a meeting date of a Sub-Group. Decision relating to MPC business will NOT be taken via this medium.

(8)   The Clerk and/or Deputy Clerk will be the sole administrators of all groups created on behalf of MPC.

(9)   Other MPC employees may also be members of groups as appropriate.

(10)   Employees will usually respond during their normal working hours but may, at their own discretion, respond at other times.

(11)   MPC Cllrs and employees have the right to request modification of the information kept on record (eg mobile phone numbers) by MPC and for their removal from any of the WhatsApp groups at any time.

(12)   MPC Cllrs and employees phone numbers must NOT be passed on via the WhatsApp group, or any other medium (eg messages must not be forwarded to phone numbers not already in the group or via any other method).

(13)   When a Cllr, or employee, leaves MPC their details will be deleted from any WhatsApp group.

(14)   MPC Cllrs and employees must ensure that any devices used for WhatsApp communication are secure, with up-to-date software and strong passwords.

(15)   MPC Cllrs and employees acknowledge that they have read and understood MPC's Privacy Notice.

(16)   Cllrs will inform the Clerk by email to confirm whether they wish their mobile number to be used for a WhatsApp group or not.

16. Misuse
(1)   Misuse of IT systems and equipment not in line with MPC's standards of conduct will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

(2)   Breach of this policy may result in the suspension of IT privileges and further consequences as deemed appropriate and/or considered a breach of the Cllrs Code of Conduct.

17. Policy Review
(1)   This policy will be reviewed annually to ensure its relevant and effectiveness. Updates may be made to address emerging technology trends and security measures.

18. Contacts
(1)   For IT-related enquiries or assistance users can contact the Parish Office on 01622 832305 or email the clerk at clerk@mardenkent-pc.gov.uk or deputy clerk at deputyclerk@mardenkent-pc.gov.uk.

(2)   Referrals can be made by the Clerk/Deputy Clerk to CloudyIT (MPC's IT support) if issues raised by Cllrs cannot be resolved.

19. Agreement of this Policy

(1)   All MPC Cllrs and staff are responsible for the safety and security of MPC's IT and email systems. By adhering to this policy MPC aims to create a secure and efficient IT environment that supports is missions and goals.

(2)   A copy of this policy is made available to all MPC Cllrs and employees. Cllrs adoption of this policy at the Annual Full Council meeting or when this document is amended constitutes their agreement to adhere to the content of this policy.

(3)   MPC officers, and any other MPC employees who use IT/social media, by signing below, agree to adhere to the content of this policy.

(4)   MPC employees, by signing this document, agree that MPC may process and share their personal information, including mobile phone number, for statutory purposes, providing information and corresponding with them in relation to the activities of the council. These details will not be passed to a third party without their prior consent.

Signed: ………………………………… (Alison Hooker – Parish Clerk)
Date:

Signed: ………………………………… (Rachel Weeks - Deputy Parish Clerk)
Date:

Signed: ………………………………… (Lisa Stevens – Administrative Assistant)
Date:

Signed: ………………………………… (Chris Prince – Village Caretaker)
Date:

Signed: ………………………………… (Neil Watkins – Parish Groundsman)
Date:

MPC employees are provided with copies of this document within their HR Employees Handbook. At 20th November 2025 grounds staff (CP and NW) only use MPC WhatsApp and cannot gain access to the administration of MPC's website or other social media platforms.

Adopted: 10th March 2026
Reviewed:
Review date: March 2027
Previously known as MPC Communications and Social Media Policy)