MESSINGHAM PARISH COUNCIL
INFORMATION TECHNOLOGY (IT) POLICY

Introduction

Messingham 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, and other authorised users.

Purpose of the IT Policy

The purpose of an IT policy is to establish clear parameters for how councillors, employees, and other authorised users, use council-provided technology or equipment, in the course of their duties. A well-defined policy helps 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.

Monitoring of IT Use

As an IT provider, the council 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.

Scope of this policy

This policy applies to all councillors, employees, 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.

Computer use

1.1 Hardware

1.1.1 Messingham Parish Council provides the Clerk with a dedicated council laptop and mobile telephone; this equipment is provided for council purposes only. Personal devices should not be used by the Clerk, for the purpose of carrying out work of the council.

1.1.2 Devices must be locked when away from the desk to prevent unauthorised access.

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

1.1.4 Computer and electronic hardware should be kept clean.

1.1.5 Equipment should not be dismantled or reassembled without seeking advice.

1.1.6 Computer or mobile equipment (including software), must not be purchased unless previously authorised.

1.1.7 Personal disks, USB stick, CDs, DVDs, data storage devices etc cannot be used on council computers without the prior approval of the council.
1.1.8 Any faults or necessary repairs must be reported to council.

Equipment

2.1 Portable equipment

2.1.1 Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.
2.1.2 It is particularly emphasised, that council back-up procedures specific to portable equipment should be followed at all times.
2.1.3 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.
2.1.4 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 council data, including emails and files, must be protected with a pin code or biometric recognition. Where possible, these devices should 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.
2.1.5 Configure devices to automatically prompt for a password after a period of inactivity of more than 30 seconds.
2.1.6 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.
2.1.7 If an item of portable equipment is lost or damaged this should be reported to the council. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet part of the loss/damage.
2.1.8 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).
2.1.9 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

2.2 Use of own devices

2.2.2 The Council recognises that councillors, may use their own smartphones, tablets, laptops etc to access council servers, for reading their emails. 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.
2.2.3 The same security precautions in this policy, apply to Councillors personal devices as to the council's desktop equipment.
2.2.4 Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.
2.2.5 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.
2.2.6 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.

2.2.7 Councillors must ensure that council related data cannot be viewed or retrieved by other people who may use the device.

2.2.8 Councillors must inform the clerk if their device(s) is/are lost, stolen, or inappropriately accessed, where there is risk of access to council data or resources.

2.2.9 Personal data relating to the council, should not be saved to any personal accounts with third-party storage cloud service providers, as this may breach data protection legislation or create a security risk if the device is lost or stolen. This applies especially if the passwords used to store/access data are saved onto the device.

2.2.10 Personal information and sensitive data should never be saved on own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

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

2.2.12 If transferring data, either by email or by other means, this should be done through an encrypted channel, such as a virtual private network (VPN) or a secure web protocol (https://). Unsecured wireless networks should not be used.

2.2.13 Prior to the disposal of any device that has council data stored on it, and in the event of a user leaving the council, users are required to allow access to the device to ensure that any identifiable data is removed from the device.

2.2.14 Councillors must take responsibility for understanding how their device(s) work in respect to the above rules, if they are accessing council servers/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 users are personally liable for their own device(s) and for any costs incurred as a result of the above.

Health and safety

3.1.1 Users who work in a council office will be provided with an appropriate workstation.

3.1.2 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.

3.1.3 Complete an annual HDE DSE Checklist to ensure the workstation is suitable – see Clerk Risk Assessment.

3.1.4 If any hazards are detected, including ‘noises’ from the IT equipment, this should be reported immediately to the council.

Password and Authentication Policy

4.1.1 All user accounts must be protected by strong, secure passwords. The council recommends following the National Cyber Security Centre (NCSC) recommendations, for 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.

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.

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.

4.1.2 Access to Passwords

- Passwords are personal and must not be shared under any circumstances.
- Only the assigned user of an account may access or use the associated password.
- 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.
- Administrative credentials must be stored securely and only accessible to authorised personnel, with a copy provided to the chair of the council in a sealed envelope, only to be accessed in an emergency.

4.1.3 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.
- Passwords must be stored using a council-approved, encrypted password manager (e.g., LastPass, Bitwarden, or KeePass).

4.1.4 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.5 Password Access Control and Logging

- All access to administrative or shared credentials must be logged and auditable.
- Attempts to access unauthorised passwords will be treated as a security incident.

4.1.6 Responsibility

- Users are responsible for creating and maintaining secure passwords for their accounts.

The IT security provider is responsible for:

- Managing system/service credentials.
- Enforcing password policies. Auditing and monitoring password-related security practices.

Monitoring

5.1.1 The council 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.

5.1.5 The council will 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.

5.1.6 Monitoring of an employee's email and/or internet use will be conducted in accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

5.1.7 The information obtained through monitoring may be shared internally, including with relevant councillors and IT employees, 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.

5.1.8 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.

5.1.9 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. Further details of these rights and how to exercise them can be found in the council's Data Protection policy.

5.1.10 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.

5.1.11 The council has software and systems in place that can monitor and record all internet usage. A daily log is kept of all activity, which details the names of all websites accessed, along with the date and time of access.

5.1.12 The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council 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.

5.1.13 Any use that the council considers to be 'improper', either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

5.1.14 All computers will be periodically checked and scanned for unauthorised programmes and viruses.

Remote working

6.1.1 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 the council's systems or services remotely, using computers that either do not belong to the council 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 device 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 for them to be kept in a locked room or cabinet;
- 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;

6.1.2 Those issued with a 'dongle' to enable internet access from a laptop via 3G or 4G networks whilst away from their normal workplace should note that the cost of internet access can be very high. Dongles should therefore be used for essential council purposes only, especially if abroad.

6.1.3 Similarly, use of paid for Wi-Fi access, for example at airports should be carefully monitored and restricted to essential council use.

Email

7.1.1 Council email facilities are intended to promote effective and speedy communication on work-related matters. Users need to be careful not to introduce viruses onto council systems.

7.1.2 All councillors and employees, who need to use email as part of their role will normally be given their own council email address and account. The council 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.

7.1.3 Email messages sent on the council's account are for council use only. Personal use is not permitted.

Use of the Internet

8.1 Copyright

8.1.1 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.

8.1.2 It is easy to copy electronically, but this does not make it any less an offence. The council's policy is to comply with copyright laws.

8.1.3 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).

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

8.2 Trademarks, links and data protection

8.2.1 The council does not permit the registration of any new domain names or trademarks relating to the council's names or products anywhere in the world, unless authorised to do so. Nor should they add links from any of the council's web pages, to any other external sites without checking first with the council.

8.2.2 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy.

8.3 Accuracy of information

8.3.1 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.

Use of social media

9.1.1 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.

All rules and breaches relating to the use of social media can be found in the Parish Council's Social Media policy and Media policy.

Misuse & Breach of this Policy

Misuse of IT systems and equipment is not in line with the council's standards of conduct and will be taken seriously.

Any inappropriate or unauthorised use by employees, may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

Failure to comply with this Policy by Councillors, will be deemed a breach of the Members Code of Conduct and will be reported to the Monitoring Officer.

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.

Notice

This document had been adapted from the specimen policy, commissioned by the National Association of Local Councils (NALC), for the purpose of its member councils and county associations.

Date Policy Adopted	9/2/2026	**Minute reference**	1926 207a)
Date of Last Review	11/5/26	**Minute reference**	1947 11m)
Date of Next Review	May 2027		