Section 1 – Annual Governance Statement 2025/26

10. We have put in place arrangements for the effective IT and data management in accordance with proper practices during the year under review.

Explanation: Milton Damerel Parish Council adopted the following IT Policy on 17th June 2016.

www.miltondamerelparishcouncil.gov.uk

MILTON DAMEREL PARISH COUNCIL

INFORMATION TECHNOLOGY (IT) POLICY

Introduction

This Information Technology (IT) Policy is based on the NALC Model IT Policy (November 2025). It sets out the rules governing the use of the Council's IT equipment and systems.

MILTON DAMEREL Parish Council operates with one employee (the Clerk), working primarily from home, using one council-owned laptop. The Council does not operate a central server, office network or shared drive.

Purpose of the IT Policy

The purpose of this policy is to:

- Set clear expectations for appropriate IT use
- Raise awareness of IT-related risks
- Safeguard Council data and digital assets
- Clarify acceptable and unacceptable use
- Outline consequences of misuse

Limited personal use of Council IT equipment by the Clerk is permitted where it does not interfere with Council duties or compromise security.

Monitoring of IT Use

As an IT provider, the Council reserves the right to monitor the use of its IT systems where there is a legitimate business reason to do so. Monitoring will be proportionate and in accordance with data protection legislation.

The Council may access files, email accounts, internet usage records and system logs where necessary for compliance, investigation, legal obligation, business continuity or system maintenance.

The Council does not currently operate continuous internet usage logging software, network traffic monitoring tools, or keystroke logging systems.

Scope

This policy applies to the Clerk and to Councillors, where relevant to the receipt or handling of Council information, regardless of their working location, or pattern, including those who are home-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.

1. Computer Use

1.1 Council IT equipment is provided for council purposes; however, reasonable personal use is permitted by the Clerk, providing it does not interrupt daily council work in any way.

1.2 The laptop must be locked when unattended, this includes from working at home or when attending other work locations, e.g. meetings. Failure to comply may lead to disciplinary action.

1.3 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.

1.4 Computer and electronic hardware should be kept clean, and every precaution should be taken to prevent food and drink from being dropped or spilt onto it.

1.5 The Council maintains an equipment record as part of its asset management.

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

1.7 Additional hardware or software must not be purchased without Council approval, unless there is a financial delegation in place.

1.8 Personal USB sticks or data storage devices, etc., cannot be used on council-owned computers without prior approval of the Chairman, and then reported to the council.

1.9 The Council does not operate internal office wireless networks.

1.10 Any faults or necessary repairs can be actioned by the Clerk under delegated financial authority, so that normal daily business may resume as soon as possible, and reported to the Chairman.

2 Equipment

2.1 Portable equipment includes the Council laptop.

2.2 All Council data must be stored within the Council laptop.

2.3 The Clerk's laptop must be stored safely and securely when not in use and should not be left unattended when working at different locations or in parked vehicles.

2.4 Devices must be password-protected.

2.5 Multi-Factor Authentication (MFA) should be enabled wherever possible.

2.6 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).

Use of Own Devices

2.7 Personal devices may be used by the Clerk to access Council email where necessary. The same security standards apply as to Council equipment.

2.8 Any emails sent from the Clerk's own devices should be sent from the Council gov.uk email account and should not identify the individual's personal email address.

2.9 Council data must not be permanently stored on personal cloud storage systems, unless authorised by the Council.

2.10 In cases of legal proceedings against the Council, the Council may need to require access to the device for the purpose of retrieving Council data.

2.11 A clear separation between the personal data processed on the Council's behalf and that processed for the user's own personal use should be maintained.

2.12 If the device supports both work and personal profiles, the work profile must always be used for work related purposes.

Personal Data

2.13 Personal data of any kind should not be saved to any personal accounts with third-party storage cloud service providers since 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, or if the service permits users to remain logged in between sessions.

2.14 Authorised users who open any attachments should ensure that any cached copies are deleted immediately after use.

2.15 Ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device.

2.16 Any work done on the user's own devices should be stored securely and password-protected and should always be backed up in accordance with the Council's standard backup procedures.

2.17 Before the disposal of any device that has work data stored on it, and in the event of the Clerk leaving the Council, the Council can request access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed.

2.18 The Clerk 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 devices. 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.

3. Health & Safety

Under Health and Safety (Display Screen Equipment) Regulations 1992 (as amended):

3.1 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.

3.2 The Clerk will be provided with appropriate workstation equipment.

4. Password and Authentication

4.1 Strong passwords must be used, as recommended by the National Cyber Security Centre (NCSC), such as the 'three random words' approach. 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 the National Association of Local Councils (NALC) guidance.

4.2 When sharing a document containing confidential information, secure link sharing should be used wherever possible. Where password-protected attachments are used, the password must be communicated separately.

4 .3 Passwords are personal data and must not be shared under any circumstances.

4.4 Only the assigned user of an account may access or use the associated password.

4.5 In exceptional circumstances (e.g. security incident, suspected data breach, or system failure), authorised personnel from an approved third party may be granted controlled access to the system or devices for the purpose of investigation, remediation or recovery. Any such access will be authorised, proportionate and documented.

4.6 Ensure that secure Wi-Fi networks are used.

4.7 Administrative credentials are held securely. A copy of the laptop passcode is retained by the Chairman in a sealed envelope for emergency access only.

4.8 Passwords must be changed immediately if compromise is suspected.

4.9 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.

5. Monitoring

5.1 The Council reserves the right to monitor computer usage and inspect any files stored on computers or associated technology, to ensure compliance with this policy as well as relevant legislation. 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.

5.2 Authorised users have 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.

5.3 The Council reserves the right to inspect all files stored on its computer systems to assure compliance with this policy.

5.4 Any use that the council considers to be 'improper' may result in disciplinary proceedings.

6. Email and Internet Use

6.1 The Council's gov.uk email account must be used for Council business.

6.2 Internet content should be treated with caution regarding accuracy and security.

6.3 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. The Clerk and Councillors are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

6.4 Email messages sent on the Council's account should be for council use only. Personal communications are permitted, provided they do not encroach upon working time or interrupt council business in any way.

7. Use of the Internet & Copyright

7.1 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 sets 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.

7.2 It is easy to copy electronically, but this does not make it any less of an offence. The Council's policy is to comply with copyright laws and not to bend the rules in any way.

7.3 It 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).

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

7.5 Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check if unsure about anything.

Trademarks, links and data protection

7.6 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 Clerk.

7.7 Special rules apply to the processing of personal and sensitive personal data.

7.8 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.

8. Use of Social Media

8.1 Care should be taken when using social media at any time on the Council's laptop.

8.2 Councillors and the Clerk must not disclose confidential information or imply they are speaking on behalf of the Council unless authorised.

8.3 The Members' Code of Conduct applies when using social media.

9. Misuse

9.1 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 may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

10. Review

10.1 This policy forms part of the Council's system of internal control and risk management arrangements and will be reviewed periodically in line with the Council's governance framework.

Adopted by the members of MILTON DAMEREL Parish Council Wednesday 17th June 2026

Proposed:

Seconded:

Signed:

Date:

Full signed document can be accessed on our documents link