Milton under Wychwood Parish Council

INFORMATION TECHNOLOGY POLICY

APPROVED AT PC ON 18/03/2026 1

SCOPE OF THIS POLICY 2

COMPUTER USE 2

1. Hardware 2

EQUIPMENT 2

1. Portable equipment 2

2.2 Use of own devices 3

PASSWORD AND AUTHENTICATION POLICY 4

MONITORING 4

REMOTE WORKING 5

EMAIL 5

USE OF THE INTERNET 6

1. Copyright 6

2. Trademarks, links and data protection 6

3. Accuracy of information 6

USE OF SOCIAL MEDIA 6

MISUSE 8

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.

Computer use

1. Hardware

1. Council computer equipment is provided for council purposes only.
2. 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.
3. Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.
4. All computer and mobile equipment will carry a number which is logged against the current owner of that equipment.
5. Equipment should not be dismantled or reassembled without seeking advice.
6. Councillors, staff, and other authorised users are not to purchase any computer or mobile equipment (including software) on behalf of the Council; that must be done through the RFO.
7. Only council owned disks, USB stick, CDs, DVDs, data storage devices can be used on council computers.
8. Any faults or necessary repairs must be reported to“the clerk.

Equipment

1. Portable equipment

1.1. Portable equipment includes laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet.

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

1.3. All portable computers must be stored safely and securely when not in use

1.4. It is important to ensure all portable devices are password protected in case they are lost or stolen.

1.5. If an item of portable equipment is lost or damaged this should be reported to the clerk.

1.6. 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).

1.7. 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. The Council recognises that some councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access our servers, private clouds or networks for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's website or to store data on the council's server(s) or access data in other services.

3. Any emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

4. 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.

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.

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.

7. Councillors, staff, and other authorised users who intend to use their own devices for the council's use must ensure that they:

- use a strong password to protect their device(s) from being accessed.
- configure their device(s) to automatically prompt for a password after a period of inactivity;
- 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 WiFi networks are used;
- ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device;
- inform the council or the clerk" 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, they will need to retain the details of their IMEI number and the SIM number of the device as their provider will require this to deactivate it.

8. Personal data relating to councillors, staff, should not be saved to any personal accounts with third-party storage cloud service providers. This applies especially if the passwords used to store/access data are saved onto the device, or if the service

permits councillors, staff, and other authorised users to remain logged in between sessions.

9. 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.

10. Councillors, staff, and other authorised users who open any attachments should ensure that any cached copies are deleted immediately after use. 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.

11. Any work done on user's own equipment should be stored securely and password protected and should always be backed up on an external device or cloud storage.

12. Prior to the disposal of any device that has work data stored on it, councillors, staff, and other authorised users are required to allow the Clerk or Chair access to the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

13. Councillors, staff, and other authorised users must take responsibility for understanding how their device works in respect to risks to the user's personal device 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.

Password and Authentication Policy

4.1.1 Access to Passwords

- Passwords are personal and must not be shared.
- Only the assigned user of an account may access or use the associated password.

4.1.2 Password Storage and Management

- Passwords must not be stored in plain text or written down in insecure locations.

4.1.3 Password Change Requirements

- Immediately change password if compromise is suspected.

4.1.6 Responsibility

- Enforcing password policies. Auditing and monitoring password-related security practices.

Monitoring

5.1.1 The council reserves the right to monitor any files stored on computers, or associated technology to ensure compliance with this policy as well as relevant legislation.

1. 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

equipment is not being abused and to protect the council from potential damage or disrepute.

2. 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.

3. All computers should 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 as follows:

- 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;
- 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;

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

Email

1. Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky. Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council equipment 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.

4. All councillors, staff, and other authorised users 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.

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

Use of the Internet

1. Copyright

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.

1. 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, and not to bend the rules in any way.

2. 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).

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

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

2. Trademarks, links and data protection

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 / the clerk.

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.

3. Accuracy of information

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

3.2. 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.

3.3. The council 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.

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 the council, or if remarks could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council 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 the council is not named, care should be taken with any views expressed.To protect both the council 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:

3.4 Contacts from any of the council'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 the council, its current work, councillors, employees, other users associated with the council, 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 the council. Writers must not claim or give the impression that they are speaking on behalf of the council.

- The council expects councillors, staff, and other authorised users to be respectful about the council and its current or potential all 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 the council's name or logo should not be posted on social media if they could reflect negatively on the individual, their role, their colleagues, or the council. 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 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 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). 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 the council or its councillors, staff, or disclose personal data or information about any individual that could breach data protection legislation.

- Contacts via the media relating to the council, should be referred to the 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 the council.
- Councillors, staff, and other authorised users who have left the council must not post any inappropriate comments about the council 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 the council, 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.

3.5. Note that the council 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.

3.6. 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.

Misuse

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.