

IT Policy

1. General

- 1.1. Reasonable personal use of Parish Council computing facilities is accepted. Personal use by employees should not interfere with the performance of your duties, cause any damage, difficulty to IT systems (including computers), or any difficulty or distress to others.
- 1.2. You should use computing facilities in a reasonable manner. You will not knowingly install any software and you should not reconfigure any machine you have access to without permission from the F&GP Committee.
- 1.3. You will not make substantial use of the Parish Council's facilities for private financial gain or for commercial purposes outside the scope of official duties or functions.

2. Internet usage (including Web browsing, Webchat)

- 2.1. You may make reasonable personal use of the Web provided it does not adversely affect your work and the work of others and has a minimal effect on the Parish Council's resources.
- 2.2. When you browse the Internet via a Web browser, you should remember the following:
 - 2.2.1. Go to known sites.
 - 2.2.2. Ensure that the padlock is shown in the URL bar indicating the site is clear when dealing with sensitive or financial transactions.
 - 2.2.3. Do not attempt to access sites that have certificate errors.
 - 2.2.4. Clear your web browser cache and cookies regularly.
 - 2.2.5. Use a VPN (virtual private network). Gives online privacy and anonymity while creating a private network from a public internet connection. (office staff).

3. Email

- 3.1 The Council reserves the right to open any Email file stored on the Council's computer system (including items stored in the Cloud).
- 3.2 When you send an Email, you should remember the following:
 - 3.2.1 Email should be regarded as written paper documents for the purposes of production, use, retention, and disclosure and can be called upon under the Freedom of Information Act 2000. Personal information should be kept in accordance with the principles established in the Data Protection Act 1998.
 - 3.2.2 Email messages can be defamatory and can and often do form contracts. For these reasons it is important to take the same care composing Email messages as letters.
 - 3.2.3 Email messages, like other documents, can be disclosed to any person mentioned in the Email under the Data Protection Act and in the event of legal proceedings.
 - 3.2.4 Messages may be seen by other people, just as postcards may be seen by postal workers. Moreover, the Parish Council cannot guarantee that communications will not be accessed illicitly.
 - 3.2.5 The privacy of any personal Email cannot be guaranteed by the Parish Council and the content may be disclosed to anyone in authority that has a valid reason to investigate or while carrying out their duties. The recommendation is that an employee must keep personal Email to essential only.
 - 3.2.6 Respect the confidentiality of information contained within Emails, even if encountered inadvertently.

- 3.3.7 Check with the sender if there is any doubt regarding the authenticity of a message.
- 3.3.8 Do not open any attachment unless certain of the authenticity of the sender.
- 3.3.9 Emails which create obligations or give instructions on behalf of the Council must be sent by officers only, not Councillors unless agreed otherwise during a meeting.

4. Security and protection of information

- 4.1 The main points to be aware of in the context of IT Systems (including computers) are:
 - 4.1.1 Ensure that antivirus and anti-malware software is up to date and correctly configured to ensure appropriate protection.
 - 4.1.2 You should guard confidential material and personal information by the proper use of a strong passwords and other security measures.
 - 4.1.3 Passwords should be complex (contain alpha, numeric, symbols and be of different case and sufficient characters, eight or more are recommended) and these must not be disclosed and ideally not written down.
 - 4.1.4 Not all computer systems are suitable for the storage of confidential information. Seek advice if you are unsure.
 - 4.1.5 Protect extremely sensitive material using encryption, i.e. 256 AES encryption.
 - 4.1.6 You must not disclose passwords or other access codes to other persons.
 - 4.1.7 You must comply with the Data Protection Act, which requires that the Parish Council keeps personal information secure.
 - 4.1.8 When working with confidential information, you must take care not to leave it inappropriately on screen. You should not leave your computer logged on when unattended unless it is in a secure location. All electronic medium must be clearly marked as such, e.g. Subject lines in Emails start "Confidential", Microsoft Word documents watermarked "Confidential".
 - 4.1.8 You should observe the same standards of confidentiality for electronically held or generated information as for information held on paper.
 - 4.1.9 All data that is stored by the Parish Council must be protected e.g. backups, encryption. All PC devices that access data and store data on site are configured with Bit Locker encryption which is 256 Bit AES.
 - 4.1.10 If you have a concern about the inadequate protection of data, you should inform the Clerk or Parish Council so that any necessary steps can be taken to safeguard the data.
 - 4.1.11 All members of staff have an obligation to protect data and systems by following up-to-date recommendations to avoid damage from viruses, other malicious programs and inappropriate use.
 - 4.1.12 When a staff member leaves the organisation, all IT system accounts will need to be revoked/withdrawn and subsequently closed.
 - 4.1.13 All access to data and cloud systems are controlled via MFA Multiple Factor Authentication.
 - 4.1.14 Teams meetings can be recorded for the purposes of producing minutes but must be deleted once the minutes have been agreed.

5. Misuse of IT Systems and Computer facilities

- 5.1 As stated above, the Parish Council permits reasonable personal as well as professional use of computing facilities. The following are not permitted:
 - 5.1.1 Hacking, the attempt to access systems or information without authority or encouraging others to do so.
 - 5.1.2 Installation of Trojans or Key loggers to covertly capture sensitive Information that may be used illicitly.
 - 5.1.3 Deliberately accessing Internet material which is contrary either to legislation, Parish Council rules or policies (e.g. equal opportunities) or to commonly accepted standards or is likely to be offensive to reasonable people. However, accidental access to such sites can take place; if you are

concerned that such accidental access has taken place you may wish to report your concerns to an appropriate person.

- 5.1.4 Email communications which constitute bullying or harassment, as defined in the Parish Council's code of advice and instructions on bullying and harassment.

6. Investigation of misuse and interception

- 6.1 The Parish Council will undertake an investigation of any suspected misuse of computing facilities and this will include accessing all files and Emails even if they are of a personal nature on all IT systems and computers that Parish Council are responsible for.
- 6.2 The following applies to Parish Council staff only:
 - 6.2.1 The Investigating Panel¹ should decide in the light of the outcome of an investigation of possible misuse of IT Systems and computer facilities whether disciplinary action is appropriate, and if it is judged appropriate, instigate necessary action in accordance with the relevant disciplinary procedures concerned.
 - 6.2.2 The Investigating Panel will report any misuse to the Finance & General Purposes Committee that will then decide whether disciplinary action should be instigated against a member of staff, making a recommendation to the Parish Council if necessary.

Adopted by Council November 2025

¹ The minimum make-up of the panel will be as follows: Chair of the PC, immediate line manager of the person being investigated, a person with an understanding of IT systems. If necessary, the council will bring in an independent person or work in partnership with a neighbouring Council.