



2026

WOOTTON PARISH COUNCIL

IT (INFORMATION TECHNOLOGY) POLICY



3 Longden Close
Haynes
Bedfordshire
MK45 3PJ

Clerk@Wootton-PC.gov.uk

Tel: 07531 930788

Version History

Version	Reviewed at	Approved at
Version 1.00	Full Council Meeting of Wootton Parish Council on 11 th March 2026	Full Council Meeting of Wootton Parish Council on 11 th March 2026
Version 1.00	Annual Meeting of Wootton Parish Council on 13 th May 2026	Annual Meeting of Wootton Parish Council on 13 th May 2026

To be reviewed at each Annual Council Meeting.

Information Technology Policy

Introduction

Wootton Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications and the need to safeguard the Parish Council's digital data and assets. This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by Councillors and employees.

Scope

This policy applies to all Councillors and employees with access to Wootton Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts. Wootton Parish Council's email accounts are to be used for official Parish Council-related activities and tasks. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

All Councillors and employees are required to confirm their acceptance of the policy content at the time of joining the Parish Council and will be asked to re-affirm their understanding and acceptance of the policy on an annual basis, by means of a resolution passed at the Annual Council Meeting.

Councillors and employees are responsible for individually complying with this policy.

Monitoring of Use

As an IT provider, Wootton Parish Council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so. Councillors and employees must be 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 Parish Council systems e.g. if they have a council e-mail address.

Wootton Parish Council aims to manage its IT systems in accordance with the principles set out in NCSC Cyber Essentials Guidance and the Practitioners' Guide 2025 (and subsequent). For fuller information see: [Cyber Essentials: Overview](#).

Computer Use

Equipment – Employees

Employees who need to use IT in their role will be provided with authorised, licensed computer equipment, software and applications for work-related tasks.

Currently, only the Clerk to the Council/Responsible Financial Officer is provided with such equipment which includes:

- Laptop.
- Two monitor screens.
- Docking station and accompanying equipment.
- Mobile phone.

Limited personal use is permitted as long as it does not violate this policy or interfere with work responsibilities. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content and the installation of unauthorised software is strictly prohibited.

Regular data backups of Parish Council devices should be performed to allow for prompt recovery of essential

services in the event of a cyber security incident. Backups will be stored to the cloud so data may be protected even if primary systems are compromised. All equipment should be kept up to date with security patches and/or updates at the earliest opportunity.

All laptops supplied should be treated with good care at all times and stored safely and securely when not in use in the office – i.e. when travelling or working away from the office. Laptops should not be left unattended nor left in parked vehicles. Laptops are expensive and damage sustained to any laptop equipment will have a financial impact on the Parish Council. Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

Equipment should not be dismantled or reassembled without seeking advice.

Employee laptops will be protected with encryption. Any security set on these devices must not be disabled or removed.

If a laptop is lost or damaged this should be reported to the Chairman and Clerk to the Council. If the loss or damage is due to an act of negligence, the individual responsible may be liable to meet the cost of repair/replacement.

Equipment - Councillors

Councillors are permitted to use their own devices, be it laptop, tablet or mobile device. Personal devices should be secured with strong passwords in accordance with the previous section, and biometric authentication where available.

Personal devices should be kept up to date with security patches.

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

Equipment – All

In all cases, Councillors and employees must lock their devices when leaving them unattended to prevent unauthorised access. Failure to comply may lead to disciplinary action.

In cases of legal proceedings, the Parish Council may need to temporarily take possession of a device, whether Council-owned or personal to retrieve the relevant data.

Email

Wootton Parish 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 and employees should take proper account of the security advice below.

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 and employees are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

These rules are designed to minimise the legal risks run when using email at work and to guide Councillors and employees as to what may and may not be done. If there is something which is not covered in the policy, Councillors and employees should ask the Chairman or Clerk to the Council, rather than assuming they know the right answer.

All Councillors and employees who need to use email as part of their role will be given their own Parish Council email address and account. The Parish 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.

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

To reduce the risk of phishing and other email threats, users should take the following precautions:

- **Be cautious of unexpected or unusual emails**, particularly those asking you to click a link, open an attachment, or provide information.
- **Check the sender's email address carefully**, not just the display name. Fraudulent emails often imitate familiar names but use incorrect or unusual addresses.
- **If an email seems suspicious, do not reply, click links, or open attachments.** Forward suspicious emails to report@phishing.gov.uk.
- **Do not trust urgent or threatening wording**, as this is often a sign of phishing attempts.

Reporting Security Incidents

Any incidents which could pose a risk to the Parish Council's systems or data security should be reported to the Clerk to the Council without delay. This includes but is not limited to:

- lost devices.
- potential risk arising from phishing emails/websites.
- passwords having been shared, and
- unauthorised third-party access to systems.

Where a security breach affects personal data, the Parish Council will follow the ICO guidance and its [Data Protection Policy](#).

Password and Authentication

All user accounts must be protected by strong, secure passwords. The Parish Council follows the National Cyber Security Centre (NCSC) recommendations for creating passwords using three random words joined with a symbol or number – such as “Beer&Chips4Me”. 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 (currently the Chairman).
- Default passwords provided by the IT provider (currently the Chairman) must be changed immediately upon installation or setup.
- Service or System (e.g. website) account passwords are generated and managed by the IT provider (currently the Chairman).
- Wootton Parish Council recommends these practices as part of its commitment to robust information security and to support compliance with 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:

- 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 Chairman, in a sealed envelope, only to be accessed in an emergency.

Password Storage and Management:

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

Password Change Requirements:

- Immediately change password if compromise is suspected.

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.

Responsibility:

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

The IT security provider (currently the Chairman) is responsible for:

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

Secure Remote Working

Increased IT security measures apply to those who work away from their normal place of work (e.g. whilst travelling), as follows:

- Avoid using public or insecure Wi-Fi for confidential Parish Council business.
- 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 Parish Council's system/services when accessible.
- Papers, files or computer equipment must not be left unattended at non-Parish Council premises unless arrangements have been made with a responsible person at non-Parish 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, Parish 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.

Retention and Archiving

Electronic records should be managed in accordance with the Wootton Parish Council's [Retention and Disposal of Documents](#). Where records contain personal data, they should be securely destroyed at the end of the retention period as outlined in the policy.

Personal data relating to Councillors, employees, associates, residents and/or external stakeholders 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.

Prior to the disposal of any device that has work data stored on it, and in the event of an employee leaving the Parish Council, employees are required to return their Parish Council-owned device to the Chairman and/or Clerk to the Council. The Chairman and/or Clerk to the Council will ensure passwords, user access shortcuts and any identifiable data are removed from the device.

Employees must take responsibility for understanding how their laptop works in respect to the above rules.

Health and Safety

Employees who work in a Parish Council office will be provided with an appropriate workstation.

The Parish 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 Wootton Parish Council's Health and Safety Policy.

Any VDU user who feels that their workstation requires changes to make it compliant must speak to the Clerk to the Council or Chairman.

If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the Clerk to the Council or Chairman.

Training and Awareness

The Clerk to the Council will advise councillors and employees of relevant training resources and opportunities, including those offered through the Bedfordshire Association of Town & Parish Councils.

Councillors are strongly encouraged to complete basic cyber security awareness training and report completion of any relevant training to the Clerk to the Council.

Use of the Internet

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 Parish Council and damages being awarded, as well as disciplinary action, including dismissal, being taken against the perpetrator.

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

Councillors and employees 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).

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

Copyright and database right law can be complicated. Councillors and employees should check with the Clerk to the Council if unsure about anything.

Trademarks, Links and Data Protection

The Parish Council does not permit the registration of any new domain names or trademarks relating to the Parish Council's names or products anywhere in the world, unless authorised to do so. No links from any of the Parish Council's web pages to any other external sites may be made without checking first with the Clerk to the Council.

Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, refer to the Parish Council's [Data Protection Policy](#).

Accuracy of Information

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

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.

Personal use of social networking/media and chat sites are not permitted during working hours.

Inappropriate comments and postings can adversely affect the reputation of the Parish Council, even if it is not directly referenced. If comments or photographs could reasonably be interpreted as being associated with the Parish Council, or if remarks about external stakeholders could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the Parish Council will treat this as a serious disciplinary offence. Councillors and employees should be aware that parishioners or other local organisations may read Councillors and employees personal weblogs, to acquire information, for example, about their work, internal Parish Council business, and employee morale. Therefore, even if the Parish Council is not named, care should be taken with any views expressed.

To protect both the Parish Council and its interests, everyone is required to comply with the following rules about social media, whether in relation to their Parish Council role or personal social networking sites:

- Contacts from any of the Parish 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 Wootton Parish Council, its current work, Councillors, employees, other users associated with the Parish Council, partner organisations, local groups, suppliers or 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 Wootton Parish Council. Even if the Parish Council 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/Wootton Parish Council". Writers must not claim or give the impression that they are speaking on behalf of the Parish Council.

- Any employee who is developing a site or writing a blog that will mention the Parish Council, current or potential plans, Councillors, employees or partners), must inform the Chairman or Clerk to the Council that they are writing this and gain agreement before going 'live'.
- Wootton Parish Council expects Councillors and employees to be respectful about the Parish Council and its current or potential employees and Councillors 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 wearing clothing displaying the Parish 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 Parish Council. Additionally, photos, videos, or audio recordings must not be taken on Parish Council premises without explicit permission.
- Comments posted by Councillors and employees on any sites should be knowledgeable, accurate and professional and should not compromise the Parish 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 or employees might be considered a breach of data protection and a breach of privacy and confidentiality. Therefore, 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 Parish Council should not be posted. This may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other Councillors, or employees, 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 and employees must be aware that they are personally liable for anything they write or present online (including on an online forum or blog, post, feed or website). Councillors should always be mindful of Wootton Parish Council's Model Code of Conduct and the Nolan Principles.
- 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 or employees 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 the Parish Council or its Councillors, employees or partners, or disclose personal data or information about any individual that could breach data protection legislation.
- Contacts by the media relating to the Parish Council, should be referred to the Clerk to the Council.
- Councillors and employees 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 Parish Council.

- Councillors and employees who use X.com, LinkedIn, or other social media/networking sites for Parish Council development purposes must ensure they provide the Parish Council with login details, including password(s), so that these sites can be accessed and updated in their absence.
- Councillors and employees who have left the Parish Council must not post any inappropriate comments about the Parish Council or its Councillors and employees on any social media/networking site.
- During your employment/ involvement with the Parish 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 or employee. All such contacts will be considered Parish Council property and may be subject to disclosure upon request.

Misuse

Councillor misuse of IT systems and equipment is not in line with the Parish Council's Code of Conduct and will be taken seriously. Any breach will be dealt with via that Code of Conduct.

Employee misuse of IT systems and equipment may lead to formal action including disciplinary proceedings or, in serious cases, dismissal.

Notes

Wootton Parish Council has a separate [Social Media, Noticeboard, Newsletter and Electronic Communications policy](#).