FRADLEY PARISH COUNCIL

IT Policy (Information Technology)

Purpose
The purpose of this policy is to establish how Councillors, Clerks, Employees, Contractors and all other users must use council-provided information technology (IT) systems, equipment, and software in a secure and lawful manner when conducting Parish Council business. It ensures compliance with statutory requirements, data protection laws, accessibility standards, and the principles of good governance.
This policy will:

- Set expectations for appropriate use of equipment and systems
- Clarify what constitutes acceptable and unacceptable use
- Raise awareness of risks associated with IT use
- Outline the consequences of policy breaches
- Safeguard the council's data and digital assets

Scope
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.

Legal and Regulatory Framework
The Parish Council must comply with:

- General Data Protection Regulation (GDPR) 2016 and Data Protection Act (DPA) 2018
- Freedom of Information Act 2000
- Transparency Code for Smaller Authorities (2015)
- Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018 (WCAG 2.2 AA standard)
- Requirements of the Annual Governance and Accountability Return (AGAR) 2025/26, Assertion 10

Email and Communication Management
The Parish Council must ensure:

- The Clerk and Council members use a generic, council-owned domain email account (e.g. clerk@parishcouncil.gov.uk)
- Personal email accounts are not used for council business
- All official communications are retained in line with the Council's Document Retention Policy
- Email messages sent on the council's account are for council use only. Personal use of a council email address is not permitted.

Website and Accessibility
The Parish Council must ensure:

- The Council's website meets WCAG 2.2 AA standards and the 2018 Accessibility Regulations
- It publishes all required information under the Transparency Code and Freedom of Information Act on its website
- Accessibility statements are published and regularly reviewed

Data Protection and Information Security
The Council is both a Data Controller and a Data Processor under the DPA 2018.
The Parish Council must ensure personal data is:

- Processed lawfully, fairly, and transparently
- Collected only for legitimate council purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Stored securely and only as long as necessary
- Access to council data must be restricted to authorised individuals
- Data breaches must be reported to the Clerk immediately and handled in accordance with ICO guidance

Use of IT Equipment and Personal Devices
Equipment owned by the council:

- Computer equipment owned by the council is provided for council purposes only
- All computers and other electronic equipment supplied by the council should be treated with good care at all times
- Equipment should not be dismantled or reassembled without seeking advice
- Councillors, staff, and other authorised users are not to purchase any computer or mobile equipment (including software), on behalf of the council, unless previously authorised
- Personal disks, USB sticks, CDs, DVDs, data storage devices etc. cannot be used on council computers
- Any faults or necessary repairs must be reported to the Chair, Vice-Chair or Clerk

Portable equipment:

- Portable equipment includes any council and personal laptops, netbooks, tablets, mobile and smart phones used for council work
- Back-up procedures specific to council-owned portable equipment should be followed at all times
- Portable equipment must be stored safely and securely; should not be left unattended when away from council premises and should never be left in parked vehicles. This is to prevent unauthorised access to data, loss and theft
- All portable devices that hold council data, including emails and files, must be protected with a pin code or strong password. Any security set on these devices must not be disenabled or removed
- If an item of portable equipment is lost or damaged this should be reported to the Chair, Vice Chair or Clerk and measures taken to protect data such as changing passwords and informing the IT administrator

Use of own devices:
The council recognises that councillors and other authorised users will use their own smartphones, tablets, laptops etc for normal council purposes, including, but not limited to, reading their emails and accessing, creating and editing documents. In these circumstances, councillors should refer and adhere to the council's data protection and retention policies in relation to the use and storage of data. Also, such devices should be kept up to date so that any vulnerabilities in the operating system or software on the device are appropriately monitored and resolved. All users must observe the following:

- Any emails sent from personal devices should be sent from a council email account and should not identify the individual's personal email address
- Where possible, users should maintain a clear separation between 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 solely be used for work-related purposes
- Councillors, staff, and other authorised users who use their own devices must ensure that they:
    a. use strong, unique passwords and (where possible) two-factor authentication
    b. configure their device(s) to automatically prompt for a password after a period of inactivity
    c. ensure secure Wi-Fi networks are used
    d. have up-to-date antivirus and security software
    e. ensure that work-related data cannot be viewed or retrieved by family or friends who may use the device
    f. inform the Chair, Vice-Chair or Clerk if their device(s) is/are lost, stolen, or inappropriately accessed and where there is risk of access to council data or resources
- Personal data relating to councillors, staff, associates, residents and 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. 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
- Personal information and sensitive data should never be saved on councillors, staff, or other authorised users own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time
- 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
- Prior to the disposal of any device that has work data stored on it and/or in the event of a user leaving the council, councillors, staff, and other authorised users must ensure that all passwords, user access shortcuts and any identifiable data are removed from the device. Assistance can be obtained from the IT administrator with this if needed
- Councillors, staff, and other authorised users must take responsibility for understanding how their own device(s) work in respect to the above rules

Software and Licensing

- Only authorised and licensed software may be installed on council-owned devices
- Cloud storage and collaboration tools must be approved by the Council
- Users must not download or use unauthorised applications for council business

Password and Authentication Policy

Password Policy:

All user accounts must be protected by strong, secure passwords. The council endorses 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 also endorsed in NALC guidance.

To further strengthen account security:

- Initial user account passwords must be generated by the IT provider
- Default passwords provided by 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 follows 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

Password Management:

- Passwords are personal and must not be shared under any circumstances
- Users are responsible for creating and maintaining secure passwords for their accounts
- Passwords must not be stored in plain text or written down in insecure locations
- Only the assigned user of an account may access or use the associated password
- In exceptional cases, access to system credentials may be granted to authorised individuals with appropriate approvals and must be logged and auditable
- Administrative credentials must be stored securely with a copy provided to the Chair in a sealed envelope, only to be accessed in an emergency
- Immediately change a password if compromise is suspected
- Attempts to access unauthorised passwords will be treated as a security incident

Monitoring and Compliance

- The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its computers or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is monitored as part of the council's protection against computer viruses, ongoing maintenance of the system and when investigating faults
- If necessary, 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
- 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
- The information obtained through monitoring may be shared with relevant councillors and also 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

- 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
- Councillors, staff, and other authorised 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. You can find further details of these rights and how to exercise them in the council's data protection policy
- 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
- 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
- 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
- Council-owned computers will be periodically checked and scanned for unauthorised programmes and viruses

Remote working

Enhanced IT security measures apply to remote working 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
- 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
- Any data should be kept safely and should 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

Use of the Internet

Copyright:

- 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
- 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
- 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)
- 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, staff, and other authorised users should check with the IT Administrator if unsure about anything

Trademarks, links and data protection:

- 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 IT Administrator
- Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy, a copy of which is on the council website or available from the Clerk

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

Social Media and Online Conduct

- 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
- 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 and/or photographs could reasonably be interpreted as being associated with the council, or 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:
    a. 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
    b. 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. Even if the 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/ the council.") Writers must not claim or give the impression that they are speaking on behalf of the council
    c. Any users who are developing a site or writing an online communication that will mention the council, must inform the Clerk and/or the Chair, that they are writing this and gain agreement before going 'live'
    d. The council expects all users to be respectful about the council and not to engage in any name calling or any behaviour that will reflect negatively on its reputation. Any unauthorised use of copyright materials, unfounded or derogatory statements, or misrepresentation is not viewed favourably and could constitute gross misconduct
    e. 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
    f. Inappropriate conversations with external stakeholders should not take place on any social networking sites, including forums
    g. 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 may include manuals; procedures; training documents; non-public financial or operational information; personal information regarding other councillors, staff, and other authorised users 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
    h. 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). Councillors should always be mindful of the Members

Code of Conduct and Nolan Principles. 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 or libellous. In addition, other users 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 council or its users, or disclose personal data or information about any individual that could breach data protection legislation.
- Contacts by the media relating to the council should be referred to the Chair or 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.
- 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 process

Training and Awareness

All Councillors, the Clerk, and employees must undertake regular training on:

- Data protection and GDPR
- Cybersecurity awareness (e.g., phishing, password management)
- Accessibility and transparency requirements

Breaches

Breaches of this policy may result in disciplinary action (where applicable) and may be reported to the Information Commissioner's Office (ICO).

Reviewed: February 2026
Next Review: May 2027