OKEFORD FITZPAINE PARISH COUNCIL

INFORMATION TECHNOLOGY POLICY

CONTENTS

This policy applies to **Okeford Fitzpaine Parish Council** and reflects that it has one PC owned laptop for use by the PC clerk. Seiretto are our website & email provider.

1. Purpose of the IT policy

The purpose of an IT policy is to establish clear parameters for how councillors and the clerk use council-provided & personal devices or equipment in the course of their duties. This policy helps to:

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

2. Monitoring of IT use

The council has the right to monitor the use of its IT equipment and systems, provided there is a legitimate reason for doing so and councillors & employees are 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 council systems e.g. if they have a council e-mail address.

3. Scope of this policy

This policy applies to all councillors & staff 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 either provided by the council or personally owned.

4. Computer use

4.1 Hardware

4.1.1 Okeford Fitzpaine PC computer equipment is provided for council purposes; however reasonable personal use is permitted (reasonable interpreted as in the opinion of the PC clerk). Any personal use of our computers and systems should not interrupt our daily council work in any way.

4.1.2 Locking computers when leaving desks - all councillors & staff must lock their computers when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work.

4.1.3 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.

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

4.1.5 All council owned computer and mobile equipment is logged against the current owner of that equipment. A record of the equipment issued will be listed on the PCs own asset register.

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

4.1.7 Personal disks, USB stick, CDs, DVDs, data storage devices should not be used on council computers. A storage device should be purchased to be used exclusively for PC business.

4.1.8 Any faults or necessary repairs must be reported to PC Cllrs as soon as possible.

4.1.9 Any PC work completed on a user's own personal computer should be stored securely with password access.

4.1.10 Prior to the disposal of any device that has council data stored on it, all passwords, access short cuts & confidential data etc should be wiped from the devices hard drive.

5. Equipment

5.1 Portable equipment

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

5.1.3 All portable computers must be stored safely and securely.

5.1.4 It is important to ensure all portable devices are protected with encryption in case they are lost or stolen. All smartphones or tablets that hold council data, including emails and files, must be protected with a pin code.

5.1.5 Any council work completed on a user's own portable device should be stored securely with password access enabled.

5.1.6 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

5.2 Use of own devices

5.2.1 The same security precautions apply to personal devices as to the council's desktop equipment. Any council business emails sent from own devices should be sent from a council email account and should not identify the individual's personal email address.

5.2.2 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.

5.2.3 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. Cllrs must ensure that work-related data cannot be viewed or retrieved by family or friends who may also use the device.

5.2.4 Cllrs must inform 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.

5.2.5 Personal information and sensitive data should never be saved on councillors or staffs own devices as this may breach confidentiality agreements, especially if the device is used by other people from time to time.

5.2.6 Any work done on a user's own equipment should be stored securely and password protected and should always be backed up in accordance with the council's standard backup procedures.

6. Health and safety

6.1 Councillors & staff who work for long periods of time using council provided equipment should ensure that their workstation is set up so that it does not cause any H&S concerns.

7. Password and Authentication Policy

7.1 All email accounts must be protected by strong, secure passwords. The council follows 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 endorsed in NALC guidance.

7.2 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 email account passwords must be generated by the email provider.
- Default passwords provided by vendors or 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 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.

7.3 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. A copy (to only be accessed in an emergency) is kept in a secure location by the clerk.

7.4 Password Storage and Management

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

7.5 Password Change Requirements

Immediately change password if compromise is suspected.

7.6 Responsibility

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

8. Email & Messaging apps

8.1 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 need to be careful not to introduce viruses onto council systems and should take proper account of the security advice below.

8.2 All councillors, staff, and other authorised users who need to use email as part of their role will 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.

8.3 Email messages sent on the council's account should be for council use only. When a Cllr resigns from office, emails sent on the PC email account will be archived/saved for future reference.

8.4 Messaging apps (e.g. WhatsApp)

- The council may use a WhatsApp group (or similar messaging app) as a convenient way of keeping councillors and the clerk informed (for example, brief updates, reminders, practical arrangements, or urgent notifications). However, WhatsApp must not be used to transact official council business or to make decisions. All official business must be conducted via council email and/or at properly convened meetings and recorded as required.
- No decisions, voting, or agreement of actions should take place via WhatsApp (including "informal" consensus). Decisions must be taken through the council's formal decision-making processes.
- Confidential, sensitive, or personal data must not be shared via WhatsApp. Where such information is necessary, use council email or other approved secure channels.
- If a WhatsApp message contains information that needs to be retained as part of the council record (for example, a complaint, instruction, decision-related discussion, or a report of a data/security incident), it must be forwarded to the clerk promptly for filing in the council's official records.

- Councillors and the clerk should be aware that information about council business held in non-corporate channels (including WhatsApp) may still be disclosable under the Freedom of Information Act 2000, even if it is on personal devices, if it is held on the council's behalf.
- Where WhatsApp is used, membership should be limited to councillors and the clerk, and the group should be administered by the clerk (or another person authorised by the council). Use should remain professional and relevant to council operations.

9. Use of the Internet

9.1 Copyright

9.1.1 Much of what appears on the internet is protected by copyright. Any copying without permission, including electronic copying, is illegal and therefore prohibited.

9.1.2 Councillors & staff 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).

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

9.1.4 Copyright and database right law can be complicated. Councillors & staff should check with the PC clerk if unsure about anything.

9.2 Trademarks, links and data protection

9.2.1 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 PC clerk.

9.2.2 Special rules apply to the processing of personal and sensitive personal data. For further guidance on this, see the council's data protection policy, a copy of which can be obtained from the PC Clerk.

9.3 Accuracy of information

9.3.1 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.

10. Use of social media

10.1 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.

10.2 The council recognises the importance of councillors & staff 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.

10.3 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 about residents/suppliers/contractors etc 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.

10.4 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:

- 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 Okeford Fitzpaine PC. 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.
- Any employee or Cllr who is developing a site or writing a blog that will mention the council, must inform The PC clerk that they are writing this and gain agreement before going 'live'.
- The council expects councillors & to be respectful about the council and its current or potential associates 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 on any sites should be knowledgeable, accurate and professional and should not compromise the council in any way.
- Any writing about or displaying photos or videos of internal activities that involves current councillors & staff 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.
- Councillors & staff 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. 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, staff, and other authorised 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 staff & Cllrs, 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 PC Clerk.
- Councillors & staff 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 who use X.com, LinkedIn, or other social media/networking sites for council development purposes must ensure they provide the council with login details, including password(s), so that these sites can be accessed and updated in their absence.
- Councillors & staff 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. All such contacts will be considered council property and may be subject to disclosure upon request.

10.5 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 and staff 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.

10.6 It is important to note that Council contact details and information remain the property of the council. In addition, councillors & staff leaving the council will be required to delete all council related data including contact details from any personal device/equipment.

11. Misuse

11.1 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.

Version no	Version date	Date adopted by Council
1.0	March 2026	May 2026