DURWESTON PARISH COUNCIL

Information Technology Policy

Table of Contents

Version Number	Version Date	Date Adopted by Council
1.0	March 2026	20th April 2026

1. Introduction

This policy applies to Durweston Parish Council and reflects that it has one laptop for use by the clerk and uses Vision ICT as its email and website provider.

2. Purpose of the IT Policy

The purpose of this IT policy is to establish clear parameters for how councillors and the clerk, use council provided technology or equipment in the course of their duties. It covers:

- 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.

3. 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 and employee 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.

4. Scope of this policy

This policy applies to all councillors and staff, regardless of their working location. It sets out the expectations for the appropriate use of IT equipment and systems provided by the council.

5. Computer use

5.1. Hardware

5.1.1. Council computer equipment is provided for council purposes only, however reasonable personal use is permitted (reasonable interpreted as in the opinion of the clerk). Any personal use of our computers and systems should not interrupt council work.

5.1.2. Locking computers when leaving desk. All councillors and staff must lock their computers when leaving their desks to prevent unauthorised access.

5.1.3. 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.

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

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

5.1.6. If removable media are used to transfer data (e.g. USB drives or CDs), it should be encrypted, the user must also securely delete the data on the media once the transfer is complete.

5.1.7. Councillors and staff 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.

5.1.8. Any work done on user's own equipment should be stored securely and password.

5.1.9. Prior to the disposal of any device that has work data stored on it, and in the event of a user leaving the council, councillors and staff are required to allow Vision ICT to access the device to ensure that all passwords, user access shortcuts and any identifiable data are removed from the device.

5.1.10. Councillors amd staff must take responsibility for understanding how their device(s) work in respect to the above.

5.2. **Software**

5.2.1. Only authorised software from legitimate sources may be loaded on to council IT equipment.

6. Equipment

6.1. Portable equipment

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

6.1.2. All portable computers must be stored safely and securely.

6.1.3. 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.

6.1.4. 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).

6.1.5. Personal data relating to councillors, staff, and other authorised users, 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.

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

6.2. Password and Authentication Policy

6.3. User email accounts must be protected by strong, secure passwords using the National Cyber Security Centre (NCSC) recommendations for creating passwords namely 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.

6.4. 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.

6.5. To further strengthen account security**:**

- Initial user email account passwords must be generated by the Vision ICT.
- Default passwords provided by vendors or the IT provider must be changed immediately upon installation or setup.
- 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.

6.6. For more guidance, see the NCSC's advice on password security: NCSC Password Guidance

6.7. **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.

6.8. **Password Storage and Management**

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

6.9. **Password Change Requirements**

- Immediately change password if compromise is suspected.

6.10. **Responsibility**

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

7. Health and safety

7.1. Councillors and staff who work for long periods using council provided IT equipment should ensure that their workstation is set up such that it does not cause any H&S concerns.

8. Email

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, and other authorised users need to be careful not to introduce viruses 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 are for council use only. Personal use is not permitted.

9. Use of the Internet

9.1. The use of the internet on council equipment is limited to legitimate council business and not for personal use.

10. Copyright

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

10.2. 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).

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

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

11. **Trademarks, links and data protection**

11.1. 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 clerk

11.2. 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 is

12. **Accuracy of information**

12.1. 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.

13. **Use of social media**

13.1. 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.

13.2. The council recognises the importance of councillors and 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.

13.3. 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 external stakeholders 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 and staff should be aware that parishioners or other local organisations may read councillors and staff 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.

13.4. 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:

- Any blog that mentions the council, its current work, councillors and staff associated with the council, partner organisations, local groups, suppliers, parishioners, should identify the author as one of its councillors or staff 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.

- The council expects councillors and staff to be respectful about the council and its current or potential staff, including employees, councillors, clerks, 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.

- 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.

- Councillors and 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.

- 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, 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 clerk.

- Councillors and 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 and staff who have left the council must not post any inappropriate comments about the council or its councillors and staff on LinkedIn, Facebook, X.com or any other social media/networking sites.

13.5. 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 clerk or Chair of the Council.

14. **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.