



Stanford in the Vale Parish Council

INFORMATION TECHNOLOGY POLICY

V1.0

March 2026

1. Introduction

This document defines the Information Technology (IT) Policy for Stanford in the Vale Parish Council ('the Council'). The Council recognises the importance of effective and secure IT and email usage in supporting its business, operations, and communications. This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, Clerk, volunteers, and contractors.

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 and other authorised users 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. Purpose and Scope

This policy, except where indicated in the text to the contrary, applies to all councillors, staff, and other authorised users. It covers all forms of information and communication technologies including council-owned devices, email systems, websites, cloud storage, and third-party platforms.

It seeks to reasonably meet the requirements of the 2025 Practitioners' Guide – Assertion 10: Digital and Data Compliance, and follow laws such as:

- Data Protection Act 2018 and UK GDPR
- Freedom of Information Act 2000
- Transparency Code for Smaller Authorities
- Website Accessibility Regulations 2018

4. Definitions

4.1. Council Computer Equipment

Refers to any computer equipment owned by the Council, including, but not limited to, PCs, peripherals such as monitors, laptop computers, netbooks, tablets, mobile and smart phones with email capability and access to the internet etc.

4.2. Remote Working

This refers to a location outside of the users' home, noting that the Council does not have any specific or dedicated offices/premises.

5. Roles and Responsibilities

- 5.1. The Clerk is responsible for managing and enforcing this policy, ensuring IT resources are used appropriately and securely.
- 5.2. Councillors and staff are responsible for complying with the policy and reporting any
- 5.3. breaches or incidents immediately.
- 5.4. External IT support providers and contractors must adhere to the standards set out in the policy when handling council information.

6. Council Computer Equipment

- 6.1. Council Computer Equipment where / if provided is for council purposes, however reasonable personal use is permitted (reasonable interpreted as in the opinion of the Council). Any personal use of our computers and systems should not interrupt our daily council work in any way.
- 6.2. All councillors, staff, and other authorised users must lock their Council Computer equipment when unattended to prevent unauthorised access.
- 6.3. Council back-up procedures specific to portable Council Computer Equipment should be followed at all times.
- 6.4. All Council Computer Equipment must be kept secure when not in use or when travelling or when Remote Working.
- 6.5. It is important to ensure all 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 or other suitable security access measure. Where possible, these devices should also be programmed to erase all content after several unsuccessful attempts to break in. Any security set on these devices must not be disabled or removed.
- 6.6. If an item of portable equipment is lost or damaged this should be reported to the Clerk.
- 6.7. 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).
- 6.8. Councillors, staff, and other authorised persons that use Council Computer Equipment are expected to use all devices in an ethical and respectful manner and in accordance with this policy.

7. Use of own devices

- 7.1. The Council permits that councillors, staff, and other authorised users may wish to use their own smartphones, tablets, laptops etc to access any council servers, private clouds or networks where available for normal council purposes, including, but not limited to, reading their emails, accessing documents stored on the council's shared drive or to store data on the council's server(s) or access data in other services.
- 7.2. Any such use of personal devices will be at the discretion of the council, but consent for standard systems (MS Windows, Mac OS X, Linux - in commercial configurations) is by default permitted to all councillors, although this permission may be withdrawn.
- 7.3. Such devices should be kept up to date so that any vulnerabilities in the operating system or other software on the device are appropriately patched or updated.

8. Password and Authentication Policy

- 8.1. Users are responsible for creating and maintaining secure passwords for their accounts (including council accounts and personal accounts used for council business where necessary).
- 8.2. Passwords should be strong.
- 8.3. Regular password changes are encouraged to enhance security.

9. Remote working

- 9.1. Increased IT security measures apply to Remote Working as follows:
 - 9.1.1. Steps should be taken to avoid messages being read by other people, including other travellers on public transport etc;
 - 9.1.2. any data should be kept safely and should only be disposed of securely;

10. Email

- 10.1. Email accounts provided by the council are for official communication only.
- 10.2. Emails should be professional and respectful in tone.
- 10.3. Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.
- 10.4. All councillors, staff, and other authorised users who need to use email as part of their role may 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.
- 10.5. Where a council email account is provided councillors are to use that account for council business rather than a personal email account.
- 10.6. Email messages sent on the council's account are for council use only. Personal use is not permitted.

11. Copyright

- 11.1. Copyright laws are to be observed.
- 11.2. Copyright and database right law can be complicated. Councillors, staff, and other authorised users should check with the Clerk if unsure about anything.

12. Trademarks, links and data protection

- 12.1. 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.

13. Use of Social Media

- 13.1. 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.
- 13.2. However, inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced.
- 13.3. 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.

- 13.4. To protect both the Council and its interests, everyone is required to comply with the following rules about social media in relation to their council role social networking sites:
- 13.4.1. 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.
 - 13.4.2. 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
 - 13.4.3. Any Councillor who is developing a site or writing a blog that will mention the Council, our current or potential plans, councillors, staff, and other authorised users, partners, must inform the Clerk that they are writing this and gain agreement before going 'live'.
 - 13.4.4. 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. 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.
 - 13.4.5. 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, 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 procedure.

14. Incident and Reporting and Cyber Security

- 14.1. Any data breach, loss of equipment or suspected cyber incident must be reported immediately to the Clerk, who will investigate and determine whether the breach needs to be reported to the Information Commissioner's Office (ICO). The Council will follow procedures outlined in its Data Protection Policy. All councillors and staff must remain vigilant against phishing attempts and other online threats.

15. Compliance and consequences

- 15.1. Breach of this IT Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

16. Policy Review

- 16.1. This policy will be reviewed annually to ensure its relevance and effectiveness.
Updates may be made to address emerging technology trends and security measures.

17. Contacts

- 17.1. For IT-related enquiries or assistance, users can contact the Clerk.
- 17.2. All staff and councillors are responsible for the safety and security of Stanford in the Vale Parish Council's IT and email systems. By adhering to this IT Policy, the Council aims to create a secure and efficient IT environment that supports its mission and goals.

Policy Owner	The Clerk
Date of Last Review	4 th March 2026
Approved by + Date	Council at Full Council Meeting 04/03/26 Minute item 22/03/26
Date of Next Review	March 2027