



INFORMATION TECHNOLOGY POLICY

1. Purpose

This policy is designed to ensure the responsible and secure use of information technology in accordance with relevant legislation, including the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025.

2. Scope

- a) This policy applies to:
 - The Parish Clerk, equipment owned by Fitzhead Parish Council (the Council); and
 - Councillors using personal devices to access, use or store Council information
- b) The Clerk is responsible for the administration and security of the Council's IT systems. Councillors are responsible for the secure use of their own devices when accessing Council information.

3. Equipment

- a) The Clerk is provided with a Council-owned laptop exclusively for official Council activities. Limited personal use is permissible, provided it does not impede work responsibilities or contravene any aspect of this policy. All usage must comply with ethical standards, respect copyright and intellectual property rights, and refrain from accessing inappropriate or offensive material.
- b) The Clerk must make sure the laptop has up-to-date antivirus protection and system updates and is routinely backed up to a secure cloud service or encrypted external device.
- a) Councillors access Parish Council information on their own devices and must keep them secure with passwords and updated software.

4. Email and Internet Use

- a) The Council utilises a .gov.uk domain, and both the Clerk and Councillors are assigned email addresses within this domain. Upon activation, these email accounts are to be used exclusively for all Council-related communications. Passwords must not be reused across personal, non-Council accounts.



- b) Once official Council email addresses are provided, personal email accounts must no longer be utilised for Council-related business.
- c) All users must be vigilant to avoid phishing and other cyber threats.

5. Data Protection and Confidentiality

- a) Any personal or special category data must be stored securely and only accessible to those with authorisation.
- b) Council users must keep their accounts and passwords secure. Strong passwords must be used and changed regularly. Login information or access rights must not be shared with unauthorised people.
- c) Council documents must not be stored unencrypted on personal devices or in personal cloud accounts.

6. Website

The Council's website, which uses the .gov.uk domain, is overseen by the Clerk.

7. Reporting

In the event of a data breach, suspected security incident, or loss of Council data, notification must be provided to the Clerk without delay, who will then action the matter as necessary.

8. Compliance

- a) To ensure adherence to this policy and applicable laws, the Council may oversee email communications. Any monitoring will only take place where necessary and will be proportionate, lawful and in accordance with Data Protection legislation.
- b) Failure to comply with this policy may result in restricted access to Council systems or other appropriate action.