OLD CLEEVE PARISH COUNCIL

INFORMATION TECHNOLOGY POLICY

Version	Date	Changes
01	16 June 2025	New Policy

1. Purpose

This policy sets out Old Cleeve Parish Council's (the Council) approach to the use of information technology (IT) resources to ensure data security, operational efficiency, and compliance with legal and regulatory obligations, including the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. Scope

This policy applies to:

- The Parish Clerk, using Council-owned equipment
- Councillors using personal devices to access, use or store Council information
- Volunteers and contractors using personal devices to access, use or store Council information.

3. Equipment

a) The Clerk is issued with a Council-owned laptop for official use. This is to be used for Council business. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All use must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

b) The Clerk is responsible for taking reasonable steps to ensure the laptop is kept secure, updated with antivirus and system patches, and backed up regularly (either to a secure cloud solution or an encrypted external device). Unauthorised installation of software, including personal software, is strictly prohibited due to security concerns.

c) Councillors currently use their own devices to access Council information. They are expected to take reasonable steps to keep these devices secure (e.g. using password protection and keeping software up to date).

4. Email and Internet Use

a) The Council operates a .gov.uk domain. The Clerk and Councillors are provided with email addresses under the domain, and once set up, these addresses must be used exclusively for all Council-related correspondence.

b) Personal email addresses must not be used for Council business once official addresses are in use.

c) All users must be vigilant to avoid phishing and other cyber threats.

5. Data Protection and Confidentiality

a) All IT use must comply with the Council's GDPR Policy and the Document Retention and Destruction Policy.

b) Any personal or sensitive data must be stored securely and only accessible to those with authorisation.

c) Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others.Users must not share login credentials or access rights with unauthorised individuals.

d) Council documents must not be stored unencrypted on personal devices or in personal cloud accounts.

6. Website

The Council website is hosted under the .gov.uk domain and is maintained by the Clerk. Any changes to the website must be approved by the Clerk or Council before being published.

7. Reporting

Any data breach, suspected security incident or loss of Council data must be reported to the Clerk immediately, who will escalate as appropriate.

8. Compliance

a) The Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

b) Failure to comply with this policy may result in restricted access to Council systems or other appropriate action.