Deeping Gate Parish Council
Information Technology Policy

To be adopted, 10th March 2026
Minute: 26.27.2.d

1. Introduction

Deeping Gate Parish Council "The Council" recognises the importance of effective and secure information technology (IT) and email in supporting its business, operations, and communications.
This policy outlines the responsibilities and required practices for Councillors, the Clerk and other authorised users (collectively "users") when using council-provided or personal devices to carry out council business.

All IT use must comply with UK GDPR, the Data Protection Act 2018, and Freedom of Information legislation.

2. Purpose

The objectives of this policy are to:

- Ensure IT systems are used appropriately and securely.
- Protect council data and digital assets.
- Define responsibilities when using council or personal devices for official duties.
- Provide guidance on secure access to council email, website, and social media.

3. Scope

This policy applies to all users accessing IT resources including:

- Computers, laptops, tablets, smartphones, and other devices
- Council networks, email accounts, software, and online platforms
- Council website and social media accounts (e.g. Facebook)

The Council maintains one laptop for the Clerk's use. Councillors use personal hardware (laptops/tablets/smart phones) for council business such as accessing emails, updating the website, and managing social media.
All users must comply with this policy to maintain security and data integrity.

4. Training and Awareness

Users must undertake IT security training provided by the Council or external sources such as:

- Parish Council Domain Helper Service virtual cybersecurity workshops

The Clerk will maintain a record of completed training and is responsible for maintaining the council laptop, including updates, backups, and security configuration.

5. Acceptable Use of IT Resources

- Council-provided IT resources must be used for official business only.
- Users must adhere to ethical standards, copyright laws, and intellectual property rights.
- Unauthorised software must not be installed without approval from the Clerk.
- IT resources must not be used to access or forward inappropriate, offensive, or illegal content.

6. Use of Personal Devices

6.1. Users must use strong, unique passwords and, where possible, enable multi-factor authentication (MFA).

6.2. Keep operating systems and applications up to date with security patches.

6.3. Use anti-virus and anti-malware software.

6.4. Ensure secure storage of council data, including emails and documents, in line with the Council's data retention and security policies.

6.5. Only access council email, website, or social media accounts through secure connections (password-protected Wi-Fi or VPN).

6.6. Users should not click on suspicious links or open unexpected attachments.

7. Password and Account Security

- Users are responsible for maintaining the security of all accounts and passwords.
- For business continuity, login details and passwords must be stored securely in an encrypted file accessible only to the Clerk, and to the Chair in the event of the Clerk's absence of emergency.
- Passwords must not be shared unnecessarily.
- Administrative credentials for council systems must be securely stored and accessible only to authorised personnel in exceptional circumstances.

8. Email Communication

- Users will be provided with official council email accounts for council business only.
- Personal email accounts must not be used for council business; Councillors and staff must use the Council-supplied .gov.uk email address.
- Emails must be professional, respectful, and comply with the Council's Code of Conduct.
- Before sending confidential or sensitive information, users must verify recipients.
- Users must be cautious when opening attachments or links; only open if the source is verified.
- All users must use the official email signature template provided by the Clerk.
- All emails sent from personal devices using official accounts are council records subject to FOI and Data Protection legislation.
- Emails sent to multiple individuals who are not official data processors must be Bcc'd to prevent the disclosure of personal data.
- The Council reserves the right to check email communications to ensure compliance with this policy and relevant laws. Monitoring will be proportionate,

targeted, and undertaken only where necessary in accordance with the Data Protection Act 2018 and GDPR.

9. Website and Social Media

- Councillors responsible for council website or social media updates must:
    - Use secure login credentials
    - Keep passwords confidential and follow all password/security rules
    - Post only professional, accurate, and authorised content
    - Avoid posting confidential council information
- Any breach of these rules must be reported immediately.

10. Data Management, Retention and Security

- All sensitive and confidential data must be stored and transmitted securely.
- Users must regularly back up important data and follow council data retention policies.
- Emails must be retained and archived in line with the Council's retention schedule.
- Unnecessary emails or files must be regularly reviewed and deleted to maintain organisation.

11. Reporting Security Incidents

- Councillors must report IT or email security incidents to the Clerk immediately, and in any event within 24 hours.
- The Clerk must report incidents to the Chair and, if necessary, the Council at the next meeting.
- The Clerk is responsible for taking appropriate steps to secure systems and notify service providers if required.

12. Compliance and Consequences

- Failure to comply with this policy may result in:
    - Restrictions on access to council IT systems
    - Escalation to the Council for review
- Serious breaches may be reported to external authorities if required by law.

13. Physical Security of Council Equipment

- The council laptop must be securely stored when not in use.
- It **must not** be left unattended in vehicles overnight.
- Serial numbers and asset information are recorded in the Council's asset register and in the secure password file.
- Users are responsible for the safe and secure use of IT systems and devices.

14. Contacts

- For IT support or security incidents:
- Councillors report to the Clerk
- Clerk reports to the Chair and Council

Users are responsible for ensuring their personal devices are secure and compliant when accessing council systems.
Monitoring of council IT systems, including email, may be conducted by the Clerk or Chair as part of policy compliance, in accordance with relevant laws.

15. Termination of Service

Upon leaving office, Councillors must:

- Delete all Council-related email accounts from their personal devices.
- Securely delete any Council documents stored locally on personal hard drives.
- The Clerk will immediately revoke access to the Council's website, social media, and email hosting.

Document History and Review			
Version	**Adoption date**	**Minute Ref.**	**Notes**
1.0	10th March 2026	26.27.2.d	First adoption

Next scheduled review: March 2027