Title:	IT Policy
Author:	Cllr Brian Flynn
Date Adopted:	4/3/2026
Version No:	v1.0
Last Reviewed:	4/3/2026
Next Review:	Annually

OSPRINGE PARISH COUNCIL: INFORMATION TECHNOLOGY POLICY

1. **Purpose**

   This policy sets out Ospringe Parish Council's 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. Its purpose is to set out parameters for the use of technology by councillors and council staff in order to perform their role. A clear policy also helps raise awareness of the risks associated with using IT and can protect the council from loss of data.

2. **Scope**

This policy applies to:

- The Parish Clerk, using Council-owned equipment and personal equipment.
- Councillors using personal devices to access, use or store Council information.
- Employees, volunteers and contractors using personal devices to access, use or store Council information.
- Publication on the council website.
- Use of Council emails and messaging services for Council business.

3. **Equipment**

a) The Clerk is issued with a Council-owned laptop and printer for official use. These devices are 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 ensuring the devices are 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 on authorised devices, 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, virus 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 same 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) Council .gov.uk email addresses must not be used for personal email.
d) Emails must be professional and respectful in tone and protect the reputation of the council.
e) All users must be cautious with attachments and links and maintain vigilance to avoid phishing and other cyber threats.

5. **Messaging**

Phone messaging and applications such as WhatsApp may be used by councillors and council staff to aid the efficient conduct of Council business, however all messaging communications must be treated in the same way as emails in terms of retention and archiving in accordance with legal and regulatory requirements.

6. **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) Parish council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security. Users must not share login credentials or access rights with unauthorised individuals.
d) Personal computers, laptops, mobile phone and other devices used to store or access Council email or data must be protected with passwords and/or biometric authentication.
e) Council documents must not be stored unencrypted on personal devices or in personal cloud accounts.

7. **Retention and Archiving**

Emails and all other council communications must be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an orderly inbox.

8. **Website and Social Media**

a) The Council website is hosted under the .gov.uk domain and is maintained by the council's designated webmaster, who is responsible for uploading/taking down content to/from the website and official Council social media accounts. Content must be factual, up to date, accurate, non-political, mindful of the Council's reputation and in line with all Council policies.

b) Only the Webmaster, Chairman and Parish Clerk can upload information to be published on the Council website or social media accounts.

c) Any significant changes to the website must be approved by the Council before being published.

d) Creation of new websites or social media accounts for Council use requires written pre-approval by the Council Chairman.

9. **Reporting**

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

10. **Training and Awareness**

The Council will provide regular access to resources to educate users about IT security best practices, privacy concerns and technology updates.

11. **Misuse of IT**

a) Misuse of IT systems is prohibited and may result in disciplinary or legal action.

b) Misuse includes but is not limited to:

- Accessing, creating or sending offensive or inappropriate content.
- Sending defamatory or infringing material.
- Distributing spam or malware.
- Interfering with others' data or work.
- Changing system settings or passwords without permission.
- Unauthorised access to or distribution of council systems, data or information.

12. **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) Compliance with this policy is to be overseen by the Council Chairman.

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

13. **Review**

This policy is to be formally reviewed annually by the Council to ensure relevance and effectiveness.

14. **Contact**

For Council IT-related enquiries or assistance, users can contact in the first instance Cllr Brian Flynn.