

Kings Hill Parish Council – Information Technology (IT) Policy

1. Purpose

This policy establishes clear standards for the use of IT systems, devices, and digital platforms by councillors, officers, and staff. It aims to ensure security, compliance with legislation, and responsible use of technology in all council activities.

2. Scope

This policy applies to:

- Council-owned devices and systems
- Personal devices used for council business
- Email, cloud services, and collaboration tools
- Remote working arrangements
- Social media and online communications

3. Principles

- Compliance with the **Data Protection Act 2018, UK GDPR**, and relevant legislation.
- Protection of council data from unauthorized access, loss, or misuse.
- Responsible and ethical use of IT resources for legitimate council purposes only.

4. Acceptable Use

- Use council-provided email accounts for official communications.
- Keep passwords secure and never share login credentials.
- Report suspected security breaches immediately to the Clerk and/or Deputy Clerk.
- Ensure devices have up-to-date antivirus software and security patches.
- Use council-approved platforms for document sharing and collaboration.

5. Unacceptable Use

- Accessing inappropriate or illegal content.
- Sharing confidential council information without authorization.
- Installing unauthorized software on council devices.
- Using IT resources for personal activities that compromise security or reputation.

6. Remote Working Guidelines

- Personal devices used for council work must have:
 - Updated antivirus software
 - Strong password protection
- Confidential documents should not be stored on personal devices unless encrypted.
- Public Wi-Fi should be avoided; if necessary, use a secure VPN.
- Video conferencing should be conducted via council-approved platforms.

7. Social Media Usage Rules

- Councillors and staff must uphold the council's reputation online.
- Official council social media accounts should only be managed by authorized personnel.
- Personal accounts:
 - Do not disclose confidential council information.
 - Avoid posting content that could bring the council into disrepute.
- All online engagement should be respectful and in line with the council's Code of Conduct.

8. Data Protection & Security

- All sensitive data must be encrypted where possible.
- Regular backups should be performed on council systems.
- Access to data should be restricted to authorized personnel only.

9. Breach of Policy

Non-compliance may result in disciplinary action and, where applicable, legal consequences.

10. Review

This policy will be reviewed annually or sooner if required by changes in legislation or council operations.

Compliance Statement

This policy supports **Assertion 10 of the Annual Governance and Accountability Return (AGAR)** and aligns with the **Practitioners' Guide** for local councils, ensuring robust governance and risk management.

Acknowledgement of Receipt and Agreement

I acknowledge that I have received a copy of the **Kings Hill Parish Council Information Technology (IT) Policy**. I have read and understood the contents of the policy and agree to comply with its terms and conditions. I understand that failure to adhere to this policy may result in disciplinary action and/or legal consequences.

Name: _____
Position: _____
Signature: _____
Date: _____