Hellingly Parish Council

IT Policy

POLICY REVIEW DATES:

NEW POLICY ADOPTED on TBA

Next review date – TBA 2027

1. Policy Introduction Statement

This policy sets out the rules and guidelines for the use, management, security, and maintenance of information technology (IT) systems, data, and devices used within Hellingly Parish Council. It aims to protect the council, its staff, councillors, and the public by ensuring that technology is used safely, effectively, and in compliance with legal and regulatory requirements.

---

2. Scope

This policy applies to:

- All employees, contractors, councillors, and volunteers using the council's IT systems or devices.
- All IT equipment (hardware), software, networks (including internet, email, and Wi-Fi), and data owned or managed by the Parish Council.
- Any personal devices used to access council IT systems or data.

---

3. Roles and Responsibilities

Role	Responsibilities
Parish Clerk	Overall responsibility for IT policy enforcement; ensures regular review and updates; approves access rights; oversees data protection and cybersecurity risks.
UniServe	Responsible for day-to-day management of the council's IT systems, including maintenance, updates, security monitoring, backups, and technical support.
Employees / Councillors / Volunteers	Read, follow and comply with this policy; use IT systems responsibly; report incidents or breaches immediately; maintain good security practices.

4. Acceptable Use

- IT systems should be used primarily for council business. Limited personal use may be permitted where it does not interfere with duties or compromise security.
- Users must not install unauthorised software or hardware.
- Email, internet, and other communication tools (i.e. mobile phones) should be used with care: no offensive, discriminatory, or illegal content.
- Passwords must be strong, kept confidential, and changed regularly as required.

- Use of portable storage (USB drives, external disks) must follow security guidelines, scanning for malware before use.

---

5. Access Control & Authentication

- Access to systems, files, and data should be granted on a “least privilege” basis: only what’s necessary for the role.
- Multi-factor authentication (MFA) should be used where available.
- User accounts must be removed or disabled promptly when no longer needed (e.g., after leaving employment or ceasing to be a councillor/volunteer).

---

6. Data Management & Protection

- All council data must be classified (e.g., public, internal, confidential) with handling rules for each class.
- Sensitive or personal data must be stored securely, encrypted where possible, and only accessed by authorised personnel.
- Regular backups of critical data must be taken, stored securely, and tested.
- Data retention schedules must be followed; data must be securely deleted/disposed of when no longer required in line with legal requirements (e.g., GDPR).

---

7. Cybersecurity & Threat Management

- Keep all software (operating systems, applications) up to date with security patches.
- Install and maintain antivirus/malware protection on all devices handling sensitive data.
- Secure the council’s network: use firewalls, VPNs (if remote access), secure Wi-Fi networks.
- Regular vulnerability assessments or audits (internally or via a third party).

---

8. Artificial Intelligence (AI)

- AI tools may be used to support council work, such as data analysis or drafting documents, but outputs must be verified for accuracy, legality, and appropriateness.
- AI must never be used to process personal data without strict compliance with data protection laws (GDPR).

- Staff and councillors must exercise caution to avoid reliance on AI for sensitive or confidential matters.
- Any AI-generated content used for official purposes must be reviewed and approved by the Parish Clerk.

---

9. Standards of Behaviour & Online Conduct

- All council policies governing behaviour, including Disciplinary Rules, Data Protection Policy, Equality & Diversity Policy, and Code of Conduct, apply equally to the use of IT systems and online activity.
- Users must conduct themselves professionally, respectfully, and lawfully when communicating via email, social media, or other digital platforms connected with council work.
- Misuse of IT systems, including harassment, bullying, discriminatory behaviour, or breaches of confidentiality, may result in disciplinary action or other measures consistent with council policies.
- Online interactions should uphold the council's values of fairness, inclusivity, and accountability.

---

10. Incident Reporting & Response

- Users must report any IT/security incidents immediately to the Parish Clerk.
- Incidents include data breaches, loss/theft of devices, unauthorised access, virus/malware infection, etc.
- The Council will maintain an **Incident Register** (see *Appendix 1*) to record, investigate, and monitor all information security, data protection, and IT-related incidents. The register will be used to ensure that all incidents are properly investigated, mitigated, and, where required, reported to relevant authorities — such as the Information Commissioner's Office (ICO) — in line with statutory and regulatory duties.

---

11. Use of Personal Devices (Bring Your Own Device – BYOD)

- Personal devices may be used only if authorised and secured (e.g., with password, encryption, malware protection).
- The council may require that certain security measures are met before granting access to council systems/data.
- If a personal device is lost, stolen, or compromised, notify the Clerk immediately; remote wipe may be required.

---

12. Training & Awareness

- All users must receive suitable training on IT security, data protection, AI use, standards of online behaviour, and this policy.
- Regular refresher training and updates on new threats, technologies, or legal changes.
- Clear guidance on best practices (e.g., phishing, safe internet use, AI verification).

---

13. Monitoring & Audit

- The council reserves the right to monitor usage of its IT systems (email, internet traffic, device logs) to ensure compliance with this policy.
- Regular audits to ensure policy adherence, security controls are effective, and any weaknesses addressed.

---

14. Policy Review & Enforcement

- This policy will be reviewed at least annually, or sooner if required by changes in law/technology or after any major security incident.
- Non-compliance with the policy may lead to disciplinary action (for employees), or other actions appropriate for councillors or volunteers.

---

15. Related Policies & Legal Obligations

This policy should be read alongside / is consistent with:

- Data Protection Policy / General Privacy Policy GDPR
- Freedom of Information Policy
- Retention & Disposal of Documents Policy
- Health & Safety General Policy
- Staff Policies: Disciplinary Policy
- Key Document: Code of Conduct
- Relevant legislation (Data Protection Act, Computer Misuse Act, etc.)

---

16. Definitions

- Personal Data: Any information relating to an identified or identifiable person.

- Sensitive (or Special Category) Data: Types of personal data that require higher protection (e.g., health, ethnicity, etc.).
- Malware: Software designed to disrupt, damage, or gain unauthorised access.
- Artificial Intelligence (AI): Computer systems capable of performing tasks normally requiring human intelligence, including data analysis, document drafting, or decision-making support.
- Online Conduct: Behaviour exhibited through emails, social media, digital collaboration platforms, or any online activity linked to council business.