Information Technology (IT) Policy

Wenvoe Community Council (WCC)

(Aligned with National Association of Local Councils (NALC) Guidance)

---

1. Purpose

This Information Technology (IT) Policy of Wenvoe Community Council (WCC) establishes the principles, standards, and controls governing the use, management, and security of the Council's information technology systems and data.

The objectives of this Policy are to:

- Ensure compliance with all applicable legal and regulatory requirements, including data protection legislation;
- Safeguard the integrity, confidentiality, and availability of Council information and IT assets;
- Promote the secure, appropriate, and effective use of technology in the conduct of Council business; and
- Support transparency, accountability, and good governance.

---

2. Scope

This Policy applies to all individuals who access or use Council IT systems, including:

- Elected Members (Councillors);
- Employees of the Council;
- Contractors, consultants, and agency staff; and
- Volunteers acting on behalf of the Council.

This Policy covers all IT equipment, systems, and services owned, leased, or used by the Council, including but not limited to:

- Desktop computers, laptops, tablets, and mobile devices;
- Email systems and Council-issued accounts;
- Cloud-based storage solutions and shared drives;
- The Council's website and social media platforms.

---

3. Roles and Responsibilities

3.1 The Council

The Council shall:

- Formally approve and periodically review this Policy;
- Ensure that adequate resources are allocated to support IT security, resilience, and compliance; and
- Promote a culture of information security and data protection.

3.2 The Clerk / Responsible Financial Officer (RFO)

The Clerk, who may also act as the Responsible Financial Officer and Data Controller (unless otherwise designated), shall:

- Oversee the implementation and enforcement of this Policy;
- Ensure compliance with relevant legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018;
- Maintain appropriate records and documentation; and
- Act as the primary point of contact for IT and data protection matters.

3.3 Users

All users of Council IT systems shall:

- Comply fully with the provisions of this Policy;
- Take all reasonable steps to protect Council data and IT equipment;
- Use Council systems in a lawful, responsible, and professional manner; and
- Report any actual or suspected IT security incidents without delay.

---

4. Acceptable Use of IT

Council IT systems are provided for the conduct of official Council business. Users shall:

- Use IT systems primarily for Council purposes;
- Refrain from accessing, storing, or transmitting material that is unlawful, offensive, defamatory, or inappropriate;
- Not install or use unauthorised software, applications, or hardware;
- Ensure that any limited personal use does not interfere with official duties or compromise security.

---

5. Email and Electronic Communications

- All Council business shall be conducted using official Council email accounts where provided;
- Personal email accounts must not be used for conducting Council business;
- Communications must be professional, lawful, and consistent with Council policies and codes of conduct;
- Care must be taken when sending sensitive or confidential information to ensure it is transmitted securely and only to authorised recipients.

---

6. Data Protection and GDPR Compliance

Wenvoe Community Council is committed to full compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Users shall:

- Access personal data only where necessary for the performance of their duties;
- Ensure that personal data is kept secure, accurate, and confidential;
- Not disclose personal data without proper authority or lawful basis;
- Adhere to the Council's data retention and disposal requirements.

Any actual or suspected personal data breach must be reported immediately to the Clerk, who will determine whether notification to the Information Commissioner's Office (ICO) is required.

---

7. Information Security

7.1 Password Management

- Strong passwords shall be used and regularly updated;
- Passwords must not be shared or disclosed to unauthorised persons;
- Multi-factor authentication (MFA) shall be implemented where available.

7.2 Devices and Systems

- All devices must be secured with appropriate access controls and locked when unattended;
- Anti-virus and security software must be installed and maintained;
- Operating systems and applications must be kept up to date with security patches.

7.3 Data Storage

- Council data shall be stored only on approved and secure systems;

- The use of personal devices for storing Council data must be authorised and appropriately secured;
- Regular backups shall be undertaken to prevent data loss.

---

8. Remote and Mobile Working

Where Council business is conducted remotely, users shall:

- Use secure and trusted internet connections;
- Avoid accessing sensitive information over public or unsecured Wi-Fi networks;
- Ensure that devices and screens are not visible to unauthorised individuals;
- Take appropriate precautions to prevent loss or theft of devices.

---

9. Website and Social Media

- All content published on behalf of the Council must be accurate, lawful, and appropriate;
- Only authorised individuals may manage or publish content;
- Accounts must be protected by strong passwords and, where possible, multi-factor authentication;
- Records of official communications conducted via social media should be retained where appropriate.

---

10. Records Management

- All records shall be created, maintained, and disposed of in accordance with the Council's Records Retention Policy;
- Electronic records must be organised, secure, and accessible for audit and transparency purposes;
- Confidential information must be securely destroyed when no longer required.

---

11. Incident Reporting and Management

All IT-related incidents must be reported immediately to the Clerk, including but not limited to:

- Personal data breaches;
- Loss or theft of devices;
- Suspected phishing attempts or malware infections;
- Unauthorised access to systems or data.

The Clerk shall assess the incident and take appropriate action, including escalation and reporting to relevant authorities where required.

---

12. Monitoring and Compliance

- The Council reserves the right, where lawful and proportionate, to monitor the use of its IT systems;
- Any breach of this Policy may result in disciplinary action and, where appropriate, legal proceedings.

---

13. Review

This Policy shall be reviewed annually, or sooner if required, to reflect changes in legislation, guidance, or operational requirements.

---

14. Adoption

This Information Technology Policy was formally adopted by Wenvoe Community Council (WCC) at a meeting of the Council held on:

Date: _____

Minute Reference: _____

Signed (Chair): _____

Signed (Clerk): _____

Appendix A: Good Practice Guidance

Users are advised to follow these good practice measures:

- Exercise caution when opening emails, attachments, or links from unknown sources;
- Verify the authenticity of requests for sensitive or financial information;
- Keep all devices physically secure at all times;
- Ensure that important data is backed up regularly in accordance with Council procedures.

Appendix B: Cyber Security Guidance (NALC/SLCC Aligned)

Wenvoe Community Council recognises the increasing risks posed by cyber threats and is committed to maintaining robust cyber security practices in line with guidance issued by the National Association of Local Councils (NALC) and the Society of Local Council Clerks (SLCC).

B1. Common Cyber Threats

Users should remain vigilant to common cyber threats, including:

- **Phishing**: Fraudulent emails or messages designed to obtain sensitive information or login credentials;
- **Malware**: Malicious software intended to disrupt, damage, or gain unauthorised access to systems;
- **Ransomware**: A form of malware that encrypts data and demands payment for its release;
- **Social Engineering**: Attempts to manipulate individuals into disclosing confidential information.

B2. Preventative Measures

To mitigate cyber risks, the Council shall implement and maintain the following controls:

- Use of up-to-date anti-virus and anti-malware software;
- Regular application of security updates and patches;
- Implementation of strong password policies and multi-factor authentication (MFA);
- Secure configuration of devices and systems;
- Routine data backups, stored securely and tested periodically.

B3. Email and Phishing Awareness

Users shall:

- Exercise caution when receiving unsolicited emails, especially those requesting sensitive information or urgent action;
- Verify the sender's identity before responding to or acting upon requests;
- Avoid clicking on suspicious links or downloading unknown attachments;
- Report suspected phishing emails immediately to the Clerk.

B4. Access Control

- Access to Council systems shall be restricted to authorised users only;
- User accounts shall be unique and not shared;
- Access rights shall be reviewed periodically and removed when no longer required.

B5. Device Security

- All Council devices shall be password-protected and encrypted where possible;
- Lost or stolen devices must be reported immediately;
- Portable devices must not be left unattended in insecure locations.

B6. Data Backup and Recovery

- Critical Council data shall be backed up regularly;
- Backups shall be stored securely and separately from live systems;
- Restoration processes shall be tested periodically to ensure data can be recovered.

B7. Incident Response

In the event of a cyber security incident:

- The incident must be reported immediately to the Clerk;
- Systems may be isolated to prevent further compromise;
- An assessment shall be undertaken to determine impact and required actions;
- Relevant authorities, including the Information Commissioner's Office (ICO), shall be notified where required.

B8. Training and Awareness

- Councillors, staff, and relevant personnel shall receive periodic cyber security awareness training;
- Users shall be kept informed of emerging threats and good practice guidance.

End of Policy