Wealden Volunteering IT and Information Security Policy

Approved by the Board: July 2026
Next Review date: July 2028

Chair Signature: 

1. Purpose

This policy sets out how Wealden Volunteering (WV) manages and protects its IT systems, digital services, and information.

It aims to:

- Safeguard personal and organisational data
- Reduce risks of cyber incidents and data loss
- Ensure systems are used safely, legally and effectively
- Support compliance with data protection and safeguarding responsibilities

All users must understand that IT security is essential to protecting the people and communities we serve.

2. Scope

This policy applies to:

- Staff, volunteers, trustees, contractors and partners
- All IT systems, devices and services used for WV business
- All access to WV systems, including remote and mobile access

3. Legal and Regulatory Framework

This policy is informed by:

- Data Protection Act 2018 & UK GDPR
- Computer Misuse Act 1990
- Data protection and cyber security guidance (ICO and NCSC)
- Charity Commission guidance on managing risk and data

4. Roles and Responsibilities

Board of Trustees

- Ensure appropriate oversight of IT risks

- Monitor compliance and risk through governance processes

CEO / Delegated Lead

- Responsible for IT systems, security, and compliance
- Responds to incidents and breaches
- Ensures appropriate controls and training are in place

All Users

All users must:

- Use systems responsibly and only for authorised purposes
- Protect passwords and devices
- Report security concerns immediately
- Comply with all organisational policies

Unauthorised use or access may result in disciplinary action and may be a criminal offence.

5. Acceptable Use of IT Systems

IT systems are provided to support WV's work and should be used primarily for that purpose.

Limited personal use is permitted where it:

- Is reasonable and infrequent
- Does not interfere with work activities
- Does not pose security risks
- Does not damage WV's reputation

WV reserves the right to restrict personal use.

Users must not:

- Engage in illegal or inappropriate online activity
- Access or share offensive, harmful or unlawful content
- Use systems for personal financial gain or external business

6. Information Security Principles

All users must:

- Only access information they are authorised to use
- Keep personal and organisational data secure
- Avoid unnecessary sharing of information
- Follow the “need to know” principle

Systems and data must be protected against:

- Unauthorised access
- Loss or theft
- Damage or corruption

7. Passwords and Access Control

- Passwords must be strong and kept confidential
- Multi-factor authentication must be used where available
- Passwords must never be shared or stored insecurely
- Access rights will be role-based and regularly reviewed

Users must:

- Lock devices when unattended
- Log out at the end of each session

Compromised passwords must be changed immediately.

8. Devices and Remote Working

Organisation devices:

- Must be kept secure at all times
- Must not be left unattended in public places
- Must be encrypted where possible

Personal devices:

May only be used with authorisation
Must meet required security standards, including:

- Up-to-date operating system and software
- Password or biometric protection enabled
- Active antivirus/anti-malware protection
- Automatic locking after inactivity

Must not store WV data locally unless permitted

Users are responsible for ensuring their personal devices remain secure and compliant.

Users working remotely must:

- Ensure secure connections
- Protect confidentiality in public/shared spaces

8.1 Removable Media

Use of removable media (e.g. USB drives, external hard drives) presents a significant security risk and must be strictly controlled.

Requirements:

- Use of removable media must be authorised by the CEO or delegated lead
- Only organisation-approved and encrypted devices may be used
- Personal USB devices must not be used for WV data
- Sensitive or personal data must not be stored on removable media unless absolutely necessary

Security Measures:

- Devices must be securely stored when not in use
- Data must be deleted securely after use
- Lost or stolen devices must be reported immediately

9. Email and Communication Security

Users must:

- Verify suspicious emails before acting
- Avoid clicking unknown links or attachments
- Not share sensitive information unless necessary

Where confidential data is shared:

- Use secure or password-protected methods where possible

Users must remain alert to phishing and fraud risks.

Phishing and Fraud Prevention
Users must take the following steps to reduce risk:

- Do not click on links or open attachments from unknown or suspicious emails
- Do not respond to requests for passwords, financial information, or sensitive data
- Always verify requests for payments or banking changes using a known, trusted contact method
- Be cautious of urgent or unusual requests, particularly those involving money or data
- Check email addresses carefully for inconsistencies or impersonation attempts

Reporting Suspicious Activity:

- Suspicious emails or messages must be reported immediately to the CEO or designated IT lead
- Do not delete suspected phishing emails until reported
- If a link has been clicked or information shared, report this immediately so action can be taken

10. Internet Use

Use of the internet must:

- Be lawful and appropriate
- Not expose WV to security threats
- Not damage WV's reputation

Users must not:

- Download unapproved software
- Access unsafe or illegal websites
- Introduce malicious software

11. Social Media

When representing WV:

- Communications must be professional, accurate and lawful
- Must not cause harm, offence or reputational damage
- Must comply with safeguarding, EDI and data protection responsibilities

Users must not share confidential or personal data via social media.

12. Data Storage and Backups

- Data must be stored in approved systems (e.g. secure cloud platforms)
- Regular backups will be maintained
- Users must not store data in unauthorised locations

Storage must align with the Data Protection Policy.

13. Data Protection and Safeguarding

IT systems must support:

- Compliance with UK GDPR
- Safe handling of personal and sensitive data
- Appropriate sharing of information where safeguarding concerns arise

Data protection must not prevent appropriate safeguarding action.

14. Monitoring and Privacy

WV may monitor use of IT systems to:

- Ensure security and compliance
- Investigate incidents
- Protect organisational interests

Monitoring will be:

- Proportionate and lawful
- In line with data protection requirements

Users should not expect complete privacy when using WV systems.

15. Data Breaches and Security Incidents

All incidents must be reported immediately to the CEO or a trustee if the CEO is absent either by email or WhatsApp or phone call. This includes suspected phishing attacks, fraudulent emails, or accidental disclosure of information

WV will:

- Investigate and assess risk
- Take appropriate action
- Report to the ICO within 72 hours where required
- Inform affected individuals where risk is high

16. Equipment Disposal

Devices and storage media must:

- Be securely wiped or destroyed before disposal
- Be handled to prevent recovery of data

17. Training and Awareness

All users will:

- Receive appropriate IT and data protection training
- Be supported to follow secure practices
- Be informed of risks and responsibilities

18. Non-Compliance

Failure to comply with this policy may result in:

- Disciplinary action
- Removal of access
- Termination of employment or volunteering
- Legal action where applicable

19. Monitoring, Review and Governance

The organisation will:

- Monitor IT risks and controls
- Review this policy every two years
- Update procedures in response to:
    - New risks
    - Cyber threats
    - Changes in law or guidance