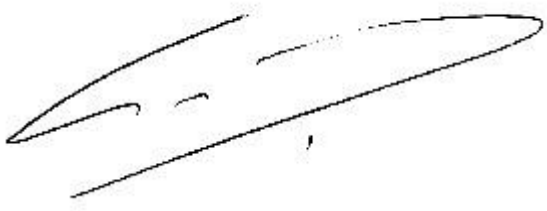
79 High Street
Uckfield
East Sussex
TN22 1AS
01825 760 919
office@wealdenvolunteering.org.uk
www.wealdenvolunteering.org.uk
Charity number: 1206210

WEALDEN VOLUNTEERING

Information Technology Policy

Date: **JULY 2024**

Review By: **DECEMBER 2026**

Chair signature: 

IT Policy

1.The Purpose of this Policy

This Policy is written to help Wealden volunteering (WV):

- reduce the risk of IT problems
- team-members, know what they can and cannot do
- protect members, service users and trustee's data
- meet our legal obligations and align with the WV Data Protection Policy

IT security problems can be expensive and time-consuming to resolve, and prevention is much better than cure. It is important that they are used responsibly, are not abused, and that individuals understand the legal, professional and ethical obligations that apply to them.

This policy applies to all team-members engaged in activities supporting and delivering WV's objectives. Team-members includes trustees, staff (whether temporary, full-time or part-time), volunteers, contractors and agents. All IT users should read this Policy in conjunction with WV's Data Protection Policy.

2. Legislation

All IT users shall comply with the relevant legislation. This includes the following:

- Data Protection Act 2018/
- Computer Misuse Act 1990
- Defamation Act 1996 and 2013
- Terrorism Act 2006
- UK GDPR 2021

3. Responsibilities and Authorisation

The Board of Trustees

The Board of Trustees are responsible for ensuring the ~~Centre~~ team-members follow and carry out the contents of this policy. The Trustees have delegated the day-to-day responsibility to the CEO. The Trustees are advised of any issues that may arise by the CEO.

The CEO may further delegate responsibility for all or parts of the IT systems. Where appropriate, references in this policy to the CEO includes someone with delegated authority. When the CEO is unavailable, the Chair or Treasurer may assume and/or delegate responsibility as needed until the CEO is available once more.

Team Members

All team-members with access to WV IT facilities (including data held in cloud-based applications) have personal responsibility for ensuring that the systems are not misused and the information is kept secure. Following the standards set out in this policy will help to fulfil this responsibility. Team members should also remain alert to anything that may indicate potential failure or misuse of the IT systems and report anything unusual without delay to the CEO or, in their absence, to the Chair or Treasurer.

No person is allowed to use the organisations IT facilities who have not previously been authorised to do so by the CEO. Unauthorised access to IT facilities is considered gross misconduct and may result in disciplinary action and/or criminal prosecution.

Team members are responsible for ensuring that all use of WV IT systems is appropriate and secure. These systems are provided to enable the work of the organisation and should be reserved for

organisational purposes. WV does permit reasonable and limited use of the IT systems for personal web browsing, checking personal email and the like but this is on the strict understanding that personal use of systems must not interfere with organisational use in any way nor bring the organisation into disrepute in any way. WV reserves the right to prohibit personal use at any time without notice or explanation. Team members should note that any information stored on WV IT systems, including usage history and data stored in the cache, is subject to inspection at any time. If team members object to inspection of their personal IT usage, they should refrain from using WV systems for personal purposes.

4. Passwords & Work Station Security

Access to WV's computer systems are secured by user passwords. Passwords must not, under any circumstances be given, or made available to others without the express and specific permission of the CEO. Team members in key roles will be granted personal access to systems. General office volunteers and others with shared roles may be given access via a shared user profile and password.

The CEO is the responsible person for changing or updating shared passwords for all equipment belonging to WV.

Users with personal access are responsible for changing and updating their own passwords. When choosing passwords, team-members should bear in mind the guidance provided by the UK National Cyber Security Centre: https://www.ncsc.gov.uk/collection/passwords

- Passwords must be at least 9 characters long. The longer the better. NCSC recommends three random but memorable words as a way of generating a long password that can be remembered.
- Avoid choosing words that are easily guessable or personal information such as memorable dates, family or pet names, favourite teams, etc.
- Avoid using the same password to access multiple systems

Passwords must never be stored in plain text either on a computer system, smart device, or on paper. NCSC strongly recommends using a password management system to store passwords securely.

Passwords should never be shared via a plain text messaging system such as email or SMS. If a password must be shared by these means, it should be considered compromised and changed immediately on receipt.

If you know or suspect that your password may be compromised or known by someone else, change it immediately. If you know or suspect that a shared password may be compromised or known by someone else, report it to the CEO, Chair, or Treasurer immediately.

Users with personal access to systems should configure and use multi-factor authentication where this is available. Users of shared profiles must not configure multi-factor authentication for those shared facilities. If muti-factor authentication is present on shared systems, the CEO will issue guidance on how to obtain the necessary authentication codes.

To prevent unauthorised access to WV's systems, users are required lock their computer whenever they are away from the screen for a brief period and to fully shutdown their computer each time they end their session.

The CEO may authorise users to carry a WV laptop and use it away from the office. Team members with laptops in their possession must always treat the device as if it contains highly valuable and sensitive information. Never leave the laptop unsecured. Use security cables where feasible to prevent opportunistic theft. Never leave the laptop or laptop case visibly in an unattended vehicle. Ideally, the laptop should either be with you or in a securely locked cabinet, room, or building at all times. Exercise caution when using a laptop in a public area (including hotels, cafes, event venues, non-WV offices, etc.) to ensure that confidential information is not accidentally displayed to people nearby.

Users must not attempt to modify or override any security setting, device, or software or any remote management or monitoring setting, device, or software provided with the workstation or cloud application. Users must not attempt to gain access to any part of the system they are not specifically authorised to

access. Users must not attempt to install any software without specific authorisation from the CEO. Any of these actions would constitute gross misconduct and may also be a criminal offence.

All WV information systems will be encrypted wherever feasible. The CEO will determine the best way to manage the secure storage of any necessary encryption keys.

All users are required to read, understand and follow stay safe online practices laminated sheet in the ~~centre~~ office on the notice board.

5. Use of the Internet

Use of the Internet is encouraged where such use is consistent with a user's work.Use of the Internet is subject to the following:

- users must not participate in any online activities that are likely to bring WV into disrepute. If you are uncertain about this, please speak to the CEO.
- users must not visit, view or download any material from an internet site which contains illegal or inappropriate material
- users must not knowingly introduce any form of computer virus into the Organisation's computer network
- users must not download commercial software or any copyrighted materials belonging to third parties
- users must not use the internet for personal financial gain, nor for illegal or criminal activities, such as software and music piracy, terrorism, fraud, or the sale of illegal drugs
- users must not use the internet to send offensive or harassing material to other users
- Users must always consider whether a site they are visiting appears to be reputable and trustworthy. Any security warnings suggesting that a site may not be trustworthy should be carefully heeded. If in any doubt, seek advice before proceeding.

6. Email Good Practice

Where sensitive and confidential information needs to be sent via email for practical reasons, please be aware that email is essentially a non-confidential means of communication. Emails can easily be forwarded or archived without the original sender's knowledge. They may be read by persons other than those they are intended for. Consider securing the sensitive information in a password protected file or using an encrypted service.

Email addresses can easily be faked. If you have doubts about whether an email really did come from the sender, then always verify before acting on any instructions in the email, opening any attachments, or clicking any links. Be especially cautious with emails that ask you to:

- Login to a website for a spurious reason (they may be directing you to a fake site to obtain your password)
- Share personal information or sensitive information
- Make a financial transaction or change information such as bank account details.

Always verify the sender (by calling, texting or using some means other than email) before doing any of these things.

WV has a virus checker on its computers, however caution must be used when opening any attachments or emails from unknown senders. Users must ensure that any file downloaded from the internet is done from a reliable source. It is a serious offence to disable the virus checker. Any concerns about external emails, including files containing attachments, must be discussed with the CEO.

Use of removable media for data storage and transfer is strongly discouraged. Where removable media is in use it must be stored securely using the same standards that would apply to paper copies of the data (eg not removed from the premises and kept in a locked cabinet) and the media must be securely erased or destroyed once that copy of the data is no longer required.

7. Use of own personal I.T equipment

Use of personal equipment to access WV IT systems, including cloud applications, is only permitted with the specific authorisation of the CEO. Users who use their own personal I.T equipment for work purposes must ensure that they are virus protected, up-to-date, and maintained to security standards similar to those in place for WV's own IT systems. In particular, users should be careful to ensure that any software downloaded or installed comes from a trustworthy source. Users must not transfer copies of WV information to their personal devices (Data that is automatically cached onto personal devices by a cloud application or a data sychronisation tool provided by the cloud storage provider is permitted).

All personal devices brought into WV are at the risk of the owner and the ~~Centre~~ WV is not responsible for any breakages or technical problems. All devices should be recharged through a power point only and never through a USB point to avoid breaching data security. Access to the centre Wi-Fi is entirely at the discretion of the CEO and subject to the same conditions as personal use of WV IT equipment including being subject to usage monitoring and withdrawal without notice or explanation.

8. Data Backups

To protect against loss of data by accidental corruption of the data or malfunction of a data storage device (including by physical damage), all WV's data shall be backed up periodically and whenever any significant changes (additions, amendments, deletions) are made to the data. Backup copies of the data are held on the Cloud which is not susceptible to common physical risks (*e g:* fire, flood, theft).

In order to ensure that data is backed up, it must be stored in the correct, authorised location. Data in the Microsoft SharePoint file shares, Microsoft Outlook, and Salesforce CRM is automatically backed up and these should be considered the default locations for storing any WV data. If there is a requirement to store information elsewhere, this must be approved by the CEO in advance.

9. Obsolete or Dysfunctional Equipment (Disposal of Removable Storage Media)

Equipment used to hold personal data, whether permanently or as interim working copies, which come to the end of their useful working life, or become dysfunctional, shall be disposed of in a manner which ensures that any residual personal data held on the equipment cannot be recovered by unauthorised persons.

In as much as:

- this will be a relatively infrequent occurrence
- techniques for data recovery and destruction are constantly evolving

Equipment which becomes obsolete or dysfunctional shall not be disposed immediately. Instead it will be stored securely while up-to-date expert advice on the most appropriate methods for its data cleansing and disposal can be sought and implemented.

10. Social Media Activities

Social media is the collective of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration. Websites and applications dedicated to forums, microblogging, social networking, social bookmarking and social curation are among the different types of social media. WV reserve the right to restrict access to these types of websites at any time

Users may be asked to contribute to the WV's social media communications and when contributing they represent WV. Where users are authorised to contribute to social media activities as part of their work, for example for marketing, promotional and recruitment purposes, they must adhere to the following rules:

- ensure that any communication has a purpose and benefit WV
- obtain permission from the CEO before embarking on a public campaign using social media
- follow all WV policies and procedures, in particular the Data Protection Policy, equality, diversity and inclusion policy, conflicts of interest policy, and the safeguarding policy

- ensure that any communication is legal, complies with the terms of the relevant social media platform, will not cause offence, harassment, or in any way bring harms the reputation of WV.

11. Monitoring

All resources, including computers, email, and voicemail are provided for legitimate use. If there are occasions where it is deemed necessary to examine data beyond that of normal business activity, at any time and without prior notice, WV have the right to examine any systems and inspect and review all data recorded in those systems. This will be undertaken at the specific instruction of the CEO, Chair or Treasurer only.

Any information stored on a computer, whether the information is contained on a hard drive, USB device or in any other manner may be subject to scrutiny by WV. This examination helps ensure compliance with internal policies and the law. It will support an internal investigation and assists in the management of information systems if necessary.

12. Contravention of this Policy

Failure to comply with any of the requirements of this policy is a misconduct (in serious cases, gross misconduct) and will result in disciplinary action being taken under the WV's disciplinary procedure.

13. Review of Policy and Procedures

WV reserve the right to update this policy at any time and will provide access to a new policy when substantial updates are completed (on the WV's website), following sign off by the Board of Trustees.

Volunteers will be notified of new policies and are responsible for ensuring they read them