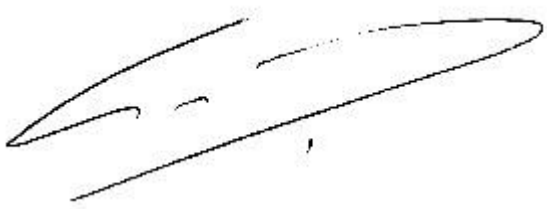
79 High Street
Uckfield
East Sussex
TN22 1AS
01825 760 919
office@wealdenvolunteering.org.uk
www.wealdenvolunteering.org.uk
Charity number: 1206210

WEALDEN VOLUNTEERING

Data Protection Policy

Approved by the Board of Trustees: JULY 2024

Review By : SEPTEMBER 2026

Chair signature: 

Data Protection Policy

1.The Purpose of this Policy

Wealden Volunteering is committed to making sure that information about service users, employees, volunteers and trustees is kept private and information is handled to all legal requirements. We recognise that people trust us to keep their information safe, and that is a responsibility that we take very seriously. This policy sets out our legal duties and responsibilities and states what we will do to ensure that we meet them.

This Policy is written in line with the requirements of the legal obligations stated below and is designed to ensure that all are aware of and meet our responsibilities towards Wealden Volunteering's (WV) personal data.

By following this Policy, the WV and its volunteers will be able to meet their legal and best practice obligations and as such reduce the risk of reputational damage or financial penalty by the Information Commissioner's Office (ICO). The ICO is the UK body responsible for monitoring compliance with data protection law and can impose penalties on organisations that are found to be non-compliant.

This policy provides information about data protection and how it applies to the WV and its volunteers, together with providing the steps to be taken by WV volunteers who have access to or store the personal data of individuals with whom the WV has or may have a relationship. This could include WV members, trustees, customers, volunteers and any individuals we deal with.

This policy applies to all trustees, staff (including agents and contractors) and volunteers engaged in activities supporting and delivering the WVs objectives. All team members should read this Policy in conjunction with WV's IT Policy.

2. Legal obligations

The UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 (DPA) govern the collection, storage and use of personal data by UK and EU organisations.

All organisations must comply with the UKGDPR and the DPA, and the potential impact of not meeting these obligations are significant fines, unlimited damages and criminal prosecution (both for the organisation and the individual concerned).

The Data Protection principles mean that, to be lawful, the collection and use of personal data that WV collects must meet the following criteria:

Area	**Detail**	**What we do at WV**
Lawfulness, fairness and transparency	Wherever personal data is collected an individual is provided with information on why we are collecting the information, what we will do with it, how long we will retain that information, etc. This is presented in the Website use policy and privacy notice which can be found on our website.	
Purpose limitation **There is always a legitimate ground to collect that data**	a) Consent (the individual wishes to be contacted) b) Contract (to fulfil a contract) c) Legal obligation (to fulfil a legal requirement)	

	d) Vital interest (to protect someone's life) e) Public interest (to perform tasks in the public interest) f) Legitimate interests to both the WV and that individual	Appendix A
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed.	
Accuracy	Personal data shall be accurate and, where necessary, kept up to date.	
Storage limitation	Personal data shall be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which they are processed.	Appendix B
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	
Accountability	WV shall be responsible for and be able to demonstrate compliance with the GDPR.	Appendix A, B & C

3. Responsibilities in the organisation

Data Controller

In UK law Data Controller is the term used for an organisation that captures, stores and uses data that identifies an individual.

Wealden Volunteering

- is a Data Controller for the processing of member, customer, volunteer and staff personal data
- as such, is responsible and accountable for the processing of personal data which is collected and used in its name
- supports the need for volunteers to have access to, and in some circumstances store the personal data of WV members and volunteers

Examples of this include access to:

- and storage of member and volunteer data to enable the administration and management of the service
- member and volunteer data to use and communicate in respect of event organisation, administration, promotion and marketing

Data Processor

Wealden Volunteering also handles some personal information provided to us by other organisations in order to carry out a specific task for them. One example of this is to carry out the grant monitoring service

for local councils. In these circumstances, we act as a Data Processor on behalf of the council who are the Data Controller.

Where we are acting as a Data Processor, we are acting under the control of the relevant Data Controller and we must only process the information in accordance with their express instructions. The relevant Data Controller's policies and procedures apply to this information rather than Wealden Volunteering's ones. We do have a legal obligation to notify any incidents or breaches to the relevant Data Controller without delay.

The Board of Trustees

The Board of Trustees are responsible for ensuring WV and its staff and volunteers follow and carry out the contents of this policy. The Trustees have delegated the day to day responsibility of data management to the CEO. The Trustees are advised of any issues that may arise by the CEO.

CEO

The CEO's role with regard to data protection is to oversee data protection standard at WV. If further information is required in respect of this privacy notice or how we handle your personal information please contact the CEO at office@Wealdenvolunteering.org.uk The CEO may choose to delegate some specific activities relating to data control at their discretion e.g. monitoring the completion of Appendix B. A review of procedures will be carried out as and when appropriate to ensure that the Policy is being adhered to and updated as necessary.

4. Processing personal data

To ensure that WV meets its legal obligations, before using or sharing personal data with individuals or organisations for usage and communications, staff and volunteers must adhere to the following:

- data protection training must be successfully completed during the relevant induction programme.
- always use corporate branding to demonstrate that the email is legitimately from WV.
- always send messages individually, taking care to ensure that email addresses are not inadvertently shared without prior agreement.
- team members should not retain lists of WV member or volunteer contact data nor retain communications or correspondence of WV members or volunteers once the purpose for which it was originally shared has been satisfied.
- Never copy information held by WV onto a personal device or personal data storage. (The use of personal devices to access WV data is permitted under certain circumstances and the copies made automatically by SharePoint/OneDrive are also permitted in these circumstances. See the IT policy for further information.)
- Never use personal information gained through your work at WV for any purpose outside of WV. If you wish to obtain contact information of another team member for social purposes, you should ask them directly for that information rather than using the information held by WV.
- Think before you share! Is it necessary to share this information? Am I allowed to share information with this person? Is this covered by WV's policy and procedures? If you cannot answer yes to all three questions, seek advice before sharing.
- always contact the CEO without delay when any issues arise related to the Rights of individuals. If the CEO is not available, contact the Chair or Treasurer. (Section 6 below)

Appendix B clarifies where personal data resides and allows us to respond to subject access requests.

It is important that data should not be transferred to a country unless it has equal levels of protection for personal data.

5. Storage of personal data

Personal data storage, which may be necessary to carry out administration of WV service must also comply with the following storage requirements:

- staff and volunteers should ensure the personal data retained is accurate, relevant and kept up to date. Out of date personal data should be removed. For example, members who have not renewed their membership should be removed from contact lists.
- the personal data can only be used for a purpose that is consistent with an individual's expectations – typically what they were told by the volunteer representing the WV when they initially provided their personal data.
- volunteers who no longer volunteer at the Centre, will have their records destroyed within 36 months of leaving the service.
- whilst retaining the personal data it must be stored according to the WV IT Policy.

6. Rights of individuals

Wealden Volunteering has an obligation to comply with the rights of individuals under the law and takes these rights seriously. The following sets out how WV will comply with these obligations:

Data Protection enquiries and requests to exercise rights

There are strict time limits to dealing with any enquiries and rights requests. If you receive any such request, it must be forwarded to the CEO without delay. If the CEO is not available, contact the Chair or Treasurer and send a copy to the CEO email address. This process applies to any request for any of the rights listed below. It applies regardless of whether the request is made formally in writing or informally by any means. If you are not sure whether a comment made by someone would be a rights request, always pass the information on so that it can be followed up.

Right to see personal information

An individual can request to see any personal information held about them by making a subject access request in writing . All information relating to the individual, including that held in electronic or manual files should be considered for disclosure.

Right to object to processing

An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest where they do not believe that those grounds are made out.

It will be assessed to whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

The CEO Officer shall be responsible for notifying the individual of the outcome of their assessment within one calendar month of receipt of the objection.

Right to rectification

An individual has the right to request the rectification of inaccurate data without undue delay. Where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual. The individual shall be given the option of a review or an appeal direct to the Information Commissioner. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed
- where consent is withdrawn and there is no other legal basis for the processing
- where an objection has been raised under the right to object, and found to be legitimate
- where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met)
- where there is a legal obligation on WV to delete.

The CEO will make a decision regarding any application for erasure of personal data and will balance the request against the exemptions provided for in the law.

Right to restrict processing

In the following circumstances, processing of an individual's personal data may be restricted:

- where the accuracy of data has been contested, during the period when WV is attempting to verify the accuracy of the data
- where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure
- where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim
- where there has been an objection made under (right to object to processing), pending the outcome of any decision

Right to portability

If an individual wants to send their personal data to another organisation they have a right to request that their information is in a structured, commonly used, and machine-readable format.

7. Third Party Access to Data

Under no circumstance will WV share with, sell or otherwise make available to Third Parties any personal data except where it is necessary and unavoidable to do so in pursuit of its objects, legal obligations, or the safety of life, as authorised by the CEO.

Whenever possible, individuals will be informed in advance of the necessity to share their personal data with a Third Party in pursuit of WV's objects.

Before sharing personal data with a Third Party, WV will take all reasonable steps to verify that the Third Party is, itself, compliant with the provisions of the GDPR and confirmed in a written contract.

The contract will specify that:

- WV is the data controller
- The Third Party will hold and process all data shared with it exclusively as specified by the instructions of WV
- The Third Party will adopt prevailing industry standard best practice to ensure that the data are held securely and protected from theft, corruption or loss
- The Third Party will notify WV without delay as soon as it becomes aware of any data breach or incident or of any request to disclose the information by a legal authority or court order.

- The Third Party will be responsible for the consequences of any theft, breach, corruption or loss of WV's data (including any fines or other penalties imposed by the Information Commissioner's Office) unless such theft, breach, corruption or loss was a direct and unavoidable consequence of the Third Party complying with the data processing instructions of the Data Protection Officer
- The Third Party will not share the data, or the results of any analysis or other processing of the data with any other party without the explicit written permission of the Data Controller
- The Third Party will securely delete all data that it holds on behalf of WV once the purpose of processing the data has been accomplished.

8. Incidents and Data Breach

An incident or data breach is when data is lost, stolen, inadvertently shared or damaged. These can happen in many ways. The most common surround human error, equipment failure or criminal activity. However, they occur, all incidents and data breaches must be reported immediately to the CEO or, if the CEO is not available, to the Chair or Treasurer.

The CEO (or a delegated officer) will follow an agreed investigating process on dealing with the incident e.g. how it happened, and whether it could have been prevented. Which includes reporting the incident to the Trustees and to the Information Commissioner's Office (if necessary) within 72 hours.

Any recommendations for further training or a change in procedure shall be reviewed and a decision made about implementation to those recommendations by the CEO.

If this Policy isn't followed WV risks being in breach of data protection law, which could result in reputational damage, fines, and court proceedings. It is better to report a potential incident that turns out not to be an issue than to risk WV facing consequences for failure to do so. Failure to report an incident without delay constitutes gross misconduct under the disciplinary policy.

9. 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 WV's website), following sign off by the Board of Trustees.

Team members are required to update their induction checklists by dating and signing that they have read the latest policies.

Appendix A
This appendix has been retired. The website use policy and privacy notice should be shared with individuals instead.

Appendix B – Completion and Storage of Data

TYPE	INFORMATION GATHERING	FILING THE FORM	REVIEW DATE
Volunteers in the centre	When a new volunteer joins the centre, they complete an application and they are required to sign and date the Induction Checklist.	The GDPR form along with their application form will be kept in the locked (four draw filing) cupboard in the centre in a *folder with their name on.*	A N N U A L L Y
Volunteers applying	Information is gathered on the volunteer application form.	. Paper forms are to be input at the Centre on the form on our website. The original paper copy to be filed in the folder and shredded after 36 months.	
Members and Trustees WV is legally obliged to share information with the Charity Commission and Companies House with basic details of WV Trustees	When a member or trustees complete the membership application form they also agree to the Privacy content.	This is a digital process and saved to the Membership file on the Trustees SharePoint. Declarations of interest form are signed annually by each trustee and filed either in the locked (four draw filing) cupboard in the centre or digitally saved on the Trustees SharePoint.	

Appendix C


How To Be GDPR Compliant
1
OBTAINING CONSENT
Your terms of consent must be clear. Consent must be easily given and freely withdrawn at any time.
2
TIMELY BREACH NOTIFICATION
If a security breach occurs, you have 72 hours to report the data breach to both your customers and any data controllers, if your company is large enough to require a GDPR data controller. Failure to report breaches within this timeframe will lead to fines.
3
RIGHT TO DATA ACCESS
If your users request their existing data profile, you must be able to serve them with a fully detailed and free electronic copy of the data you've collected about them. This report must also include the various ways you're using their information.
4
RIGHT TO BE FORGOTTEN
Also known as the right to data deletion, once the original purpose or use of the customer data has been realized, your customers have the right to request that you totally erase their personal data.
5
DATA PORTABILITY
This gives users rights to their own data. They must be able to obtain their data from you and reuse that same data in different environments outside of your company.
6
PRIVACY BY DESIGN
This section of GDPR requires companies to design their systems with the proper security protocols in place from the start. Failure to design your systems of data collection the right way will result in a fine.
7
POTENTIAL DATA PROTECTION OFFICERS
In some cases, your company may need to appoint a data protection officer (DPO). Whether or not you need an officer depends upon the size of your company and at what level you currently process and collect data.
core dna