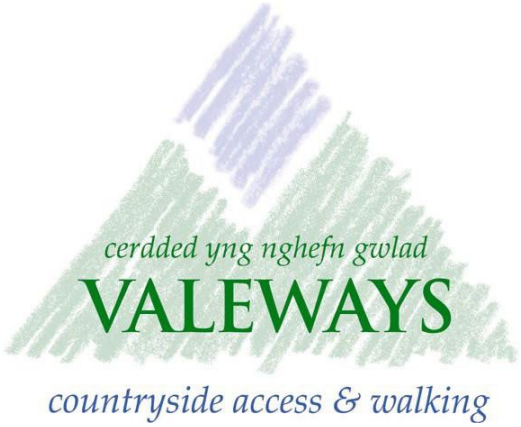

VALEWAYS

Security Policy

(including Data Security and Document Management)

1. PURPOSE and SCOPE

VALEWAYS is committed to meeting its obligations under current legislation. VALEWAYS will strive to observe the law in all collection and processing of subject data and will meet any subject access request in compliance with the law. VALEWAYS will only use data in ways relevant to carrying out its legitimate purposes and functions as a charity in a way that is not prejudicial to the interests of individuals. VALEWAYS will take due care in the collection and storage of all personal data. VALEWAYS volunteers will do their utmost to keep all data accurate, timely and secure.

All VALEWAYS volunteers must be aware of the requirements of the current legislation when they collect or handle data about an **individual**. VALEWAYS volunteers must not disclose data except where there is subject consent, or legal requirement. All collection and processing must be done in good faith.

The General Data Protection Regulation (GDPR) imposes statutory conditions for the maintenance of personal data on VALEWAYS computer systems including data held by individual volunteers on their own devices. It is an offence to use or disclose such data if not registered to do so under the GDPR. Staff may use or store work related data on their own devices at home for VALEWAYS purposes only.

VALEWAYS will keep records of all complaints by data subjects and the follow up. It will also keep a record of all data access requests and information about any contacts made with the Information Commissioner. This information will be available to staff and data subjects on request.

VALEWAYS will inform subjects of any processing, disclosure or overseas transfer that does not fall within VALEWAYS' purpose in a way that any individual supplying could be expected to understand. VALEWAYS will keep registration (now called notification) up to date.

2. PRINCIPLES of DATA PROTECTION (as outlined in GDPR)

Anyone processing personal data must comply with the following principles of good practice, which VALEWAYS seeks to uphold. The principles say that data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not be processed in a way that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Not kept longer than necessary for the purposes for which the data are processed;
- Processed in a manner that ensures appropriate security of the data (including to prevent unauthorised or unlawful processing, accidental loss, destruction or damage) using appropriate technical or organisational measures.
- Must not be transferred outside of the EEA (European Economic Area) unless the country has an adequate level of protection for data subjects.

3. POLICY on COLLECTION of SUBJECT DATA

VALEWAYS will only collect data that is relevant to the carrying out of the legitimate purposes and functions of the charity in a way that is not prejudicial to the interests of individuals. All data on individual subjects will be treated in a consistent way. Subjects will be informed about how VALEWAYS will store and use the data at the time of collection. This will require a standard statement to be sent in all written requests for data and a similar verbal script to be used for phone data collection.

Where the contact details (address, telephone number, email, etc) of an organisation are those of a private individual rather than office premises, those details will be considered to be personal data.

Where VALEWAYS intends to use personal data for its main purposes, sending information, newsletters or mailings, subjects will be made aware of their rights and be required to give consent. The obtaining of consent will abide by the following principles:

- Consent requires an active **opt-in.** – e.g. unticked opt-in boxes or similar active opt-in methods (e.g. yes/no).
- Consent needs to be specific and granular – vague or blanket consent is not appropriate or acceptable.
- VALEWAYS will name any third parties who will rely on the consent.
- VALEWAYS will keep consent requests separate from other terms and conditions.
- VALEWAYS will avoid making consent a precondition of a service.

VALEWAYS will strive to ensure that data collection is as accurate as possible, given the methods used in collection. Voicemail data may be less reliable than written documents. Data may be stored in many ways. The data will be collected consistently no matter where the data is to be stored.

4. SENSITIVE DATA

VALEWAYS will strive to ensure that sensitive data is accurately identified on collection so that the proper safeguards can be put in place. Sensitive data means data consisting of information relating to the individual's:

a) Racial or ethnic origin
b) Political opinions
c) Religious or philosophical beliefs
d) Trade Union
e) Health
f) Sex life or sexual orientation
g) Civil or Criminal offences.

5. PROCEDURE for COLLECTION of SUBJECT DATA

Volunteers are responsible for ensuring that data is collected accurately and fully.

Volunteers are responsible for ensuring that sensitive data is identified when collected and will inform the subject that this data will be stored at the time of collection.

All personal information should be dated at the time of collection so that records can be archived at an appropriate time.

6. STATEMENT for COMMUNICATIONS (written forms and web/email)

When data is collected the following statement must be included in all written forms and also electronic communications:

"If you complete this form VALEWAYS will store and process your data in accordance with the requirements of its **Security Policy** and in keeping with GDPR. As part of our commitment to keeping you informed, VALEWAYS would like to send information to you from time to time including but not limited to our newsletter, e-bulletins, invitations to events. **Please tick the box if you consent to receiving information from VALEWAYS in this way."**

7. POLICY for DATA STORAGE and PROCESSING

VALEWAYS will only hold data that is relevant to the carrying out of the legitimate purposes and functions of the charity in a way not prejudicial to the interests of individuals. Information will be accurate and timely and will be held in an environment as secure as possible. VALEWAYS volunteers will be responsible for ensuring that all regular data care procedures are fully and conscientiously followed. All ordered manual files and databases will be kept up to date and will have an agreed archiving policy. Data no longer required for the legitimate purposes of VALEWAYS will be regularly purged.

All individual data will be kept secure, by regular office security procedures or through the controls over the computer network. Sensitive data will be treated with appropriate security.
Volunteers will also take care to meet high standards of security by disposing appropriately any written reports, which are generated from individual records. Any data processing will only be allowed where there is a clear rationale for the activity, which meets the GDPR criteria.

8. PROCEDURE for DATA STORAGE and PROCESSING

- All volunteers must take responsibility for following through any data care work required of them to maintain accurate corporate data systems. They are also responsible for any records they keep in any ordered filing systems.
- Archiving policies for data no longer needed in our storage systems will be set up for all data stores. A clear rationale must be supplied for personal data to be kept beyond longer than is necessary.
- All data will be stored in a secure location and precautions will be taken to avoid letting data become accidentally disclosed.
- Any agent employed to process data on VALEWAYS' behalf will be bound to comply with VALEWAYS' Security Policy by a written contract. No data will passed to a Third Party without obtaining consent of the data subject.
- Any mailings generated from stored data will observe opt out choices in good faith.
- Sensitive data should not be kept unless agreed by the Data Controller at VALEWAYS. The position of Data Controller will default to the Chair of Trustees unless the duties are formally delegated.
- Information that is stored on computers, mobile devices and laptops will be password protected. However, as with Archiving Procedures (qv, tba), the necessity for password protection will be defined by the document owners.

9. POLICY on DISCLOSURES

VALEWAYS will not allow data collected from subjects to be disclosed to third parties except in circumstances that meet the requirements of the General Data Protection Regulation.

This will be either:

- The subject has consented to the disclosure.
- VALEWAYS is legally obliged to disclose the data.
- There is a business requirement to disclose data that is within the remit of GDPR and is not prejudicial to the interests of the individual.

Any request for data based on a legal requirement, e.g. from Police or other body, must be put in writing and be checked against the advice of the Information Commissioner Registrar before data are disclosed.

All volunteers have a duty to protect individuals' data from accidental disclosure:

- Do not give out passwords to other people, who will then have access to the data you are entitled to view.
- Do not recycle reports that contain personal data.

- In particular, take due care to ensure that data is not left about on laptops or mobile devices or in files out of the office where they can be accessed by other people who are not VALEWAYS staff.

10. POLICY on OVERSEAS TRANSFER

VALEWAYS will not allow data collected from subjects to be transferred to third parties outside of the European Economic Area except in circumstances which meet the requirements of the General Data Protection Regulation. This will be either:

- The subject has consented to the transfer.
- VALEWAYS is legally obliged to transfer the data.
- There is a business requirement to transfer the data that is within the remit of the Data Protection Law as it is not prejudicial to the interests of the individual.

Any data put on the Internet, via emails or Web Page will be considered a data transfer.

Any request for data based on a legal requirement, e.g. from Police or other body, must be put in writing and be checked against the advice of the Information Commissioner before data is transferred Overseas.

11. SUBJECT ACCESS POLICY

All data subjects have the right to request a copy of all personal data held by VALEWAYS relating to the data subject. This information must be provided within 1 month (at the latest) but may be extended where requests are complex or numerous. This information must also be provided **free of charge**. However, VALEWAYS may charge a "reasonable fee" if the request is manifestly unfounded or complex. If a request is made electronically, the information may be provided in a commonly used electronic format.

Exceptions

In certain circumstances, the disclosure of data will involve disclosing information relating to another individual. In such cases, VALEWAYS will not be obliged to disclose the information unless the other individual has consented to the disclosure or it would be reasonable in all the circumstances to comply with such a request without such consent. These will be:

- Where the data controller is involved in negotiations with the data subject, the subject access provisions will not apply if their application would prejudice the negotiations
- Any personal data which is processed by the data controller for the purpose of management forecasting or management planning done in the conduct of VALEWAYS' business, will be exempt from the subject access provisions if such access would be likely to prejudice the conduct of such business or activity
- Where legal professional privilege can be claimed, the subject access provisions will not apply.

12. NOTIFICATION of BREACH

VALEWAYS is required to notify a personal data breach to the Information Commissioner as the supervisory authority if the breach is likely to result in risk to rights and freedoms and

individuals. Where feasible, all breaches must reported no later than 72 hours after becoming aware of the breach. Examples of breaches include (this list is not exhaustive):-

- Loss or theft of memory stick/pen drive containing personal data.
- Loss or theft of a mobile device containing personal data.
- Loss or theft of manual files containing personal data.
- Inadvertently sending personal data electronically.

All VALEWAYS staff **MUST** report a suspected breach to the data controller immediately and as a matter of urgency. Failure to report a suspected breach will result in disciplinary action being taken. The Data Controller will record the breach and decide whether the Information Commissioner should be notified.

Definitions

Data controller is the person (either alone or jointly with other persons) who determines the purposes for which and the manner in which personal data is processed. VALEWAYS' data controller is, by default, the Chair of Trustees unless and until the responsibility is formally delegated.

Data Protection Principles: all data must be processed in accordance with the data protection principles, as detailed previously.

Manual data: is data that is held on "a relevant filing system" with the intention that it should form part of such a system. A "relevant filing system" is any set of information relating to individuals which is "structured either by reference to individuals or by reference to criteria relating to such individuals" so that such information is "readily accessible".

Personal data means data consisting of information that relates to a living individual who can be identified from the information, or from that and other information in the possession of the controller. Expressions of opinion about an individual also constitute "personal data" but any indications of the intentions of the data controller in respect of that person do not. The facts on which such "intentions" are formulated, e.g. performance ratings, count as personal data and must be disclosed on request to the data subject.

Processing includes obtaining, holding and recording data. In practice, it will mean that anything done to data will be processing.

Sensitive personal data is personal data relating to the individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, commission or the alleged commission of an offence, or proceedings relating to such an offence.

Approved Jul7 2021
Reviewed and revised February 2024