Volunteer It Yourself Data Protection Policy

Document	**Data Protection Policy**
Date of original document	**May 2018**
Original document author	**Ottolien van Rossem**
Latest document revisions	**December 2023**
Revised by	**Ed Sellwood, Alex Berwick**
Approved by	**VIY Board**
Next review date	**November 2024**

Policy statement

This Data Protection Policy applies to personal information that we, Volunteer It Yourself (VIY), collect about individuals who interact with our organisation. It explains how we handle personal data and makes sure that it is protected.

Data protection principles

We are committed to processing data in accordance with our responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- 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

General provisions

- This policy applies to all personal data that we process
- The Responsible Person shall take responsibility for VIY's ongoing compliance with this policy
- This policy shall be reviewed at least annually
- VIY is registered with the Information Commissioner's Office as an organisation that processes personal data

Lawful, fair and transparent processing

- To ensure our processing of data is lawful, fair and transparent, VIY shall maintain a Register of Systems
- The Register of Systems shall be reviewed at least annually

- Individuals have the right to access their personal data and any such requests made to us shall be dealt with in a timely manner

Lawful purposes

- All data that we process must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests
- We shall note the appropriate lawful basis in the Register of Systems
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data
- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in our systems

Sharing information

We will not sell or rent your data, and do not swap data with anyone.

We are committed to protecting your data and therefore it will never be disclosed to external organisations other than those acting as agents and data processors carrying out work on our behalf.

Where we enter into a relationship with any external party, any such arrangements will be subject to a formal agreement between VIY and that organisation to protect the security of your data.

Examples of where we may share your data include when:

- We enter into a funding contract with a Local Authority
- We report to funders and other partners on the impact of their donation to the young people we help
- We use case studies to promote our organisation and brand
- We work with external parties to develop our Customer Relationship Management systems
- We work with Lead Mentors who will be working with the young people on the VIY project
- We work with City & Guilds when a young person has achieved a City & Guilds qualification

Data minimisation

- We shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Where data is collected on the basis of consent, we will seek renewal of consent at least every three years
    - Where it is not possible to renew consent for the storage of personal data:
        - Data will be pseudonymised if it is required for evaluation purposes
        - Data will be anonymised if it is not required for evaluation purposes
- For the purpose of the City & Guilds accreditation we are required to store the data for five years and we will delete that data promptly once it is no longer required

Accuracy

- We shall take reasonable steps to ensure personal data is accurate
- Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date

Archiving / removal

- To ensure that personal data is kept for no longer than necessary, we shall put in place archiving procedures for each area in which personal data is processed and review this process annually
- The archiving procedures shall consider what data should/must be retained, for how long, and why

Security

- We shall ensure that personal data is stored securely using modern software that is kept up-to-date
- Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information
- When personal data is deleted this should be done safely such that the data is irrecoverable
- Appropriate back-up and disaster recovery solutions shall be in place

Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, we shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.

When we are using online platforms to communicate with children and young people

We do, from time to time, use online platforms to communicate with children and young people. As mentioned in our Child Protection & Safeguarding Policy, we will always have two team members present during these sessions.

Based on advice from VIY partners, we will not be recording, either audio or video, any of these sessions.

We are however aware that this situation may change if, for instance, a project partner or funder requests a copy of our sessions as evidence that they have taken place. In the event of this happening, we will have procedures in place across the following:

- Why we are recording audio/video content
- What we will do with the recordings
- How long we will store the recordings for
- Where we will store the recordings
- What the process is for deleting the recordings when we no longer need them
- Who will have access to the recordings (which will be password protected)
- How a young person, parent or carer can contact us if they would like the content deleted (and who is responsible for deleting it)