DVC Data Protection Policy 2018

1. What data DVC keeps and why it keeps this data.

DVC holds personal data in order to provide the best possible service to the individuals and organisations who access our projects and services. Data includes personal information that is used to match potential volunteers with volunteering opportunities, information that helps us to identify the health & wellbeing requirements of local people, and organisational contact details.

Where we process special category data we rely on explicit consent. This means that if we are asking you to give us information on your health, ethnic origin or other sensitive data then we will ask you to consent to us processing your data and we'll tell you what we will be using it for.

We won't share your personal information with third parties unless you give us your permission, ask us to or expect us to as part of the service we're giving you. Examples of when we might share your data are: when we're helping you find a volunteering opportunity, or referring you on to another organisation for more support or another service.

If we share your data with another organisation then we will always do our best to keep it secure.

In exceptional circumstances we may share your personal information without your permission if we reasonably believe:

- your health or safety is at risk
- if we believe you might be breaking the law,
- and where such a disclosure is allowed under the relevant laws, including data protection law.

We often report to funders and other bodies on our performance of services. When we do this we will anonymise the data we provide unless you have given us explicit consent to share your information.

Approved by Management Committee 01/06/2018

2. To what types of data the policy applies.

This policy applies to the following personal data collected by DVC which covers staff, volunteers and Trustees:

- **Biographical information or current living situation**, including dates of birth, Social Security numbers, phone numbers and email addresses.
- **Workplace data and information about education**, including salary, tax information and student numbers (staff).
- **Private and subjective data**, including religion
- **Health, sickness and genetics**, including medical history, genetic data (age, disabilities, ethnicity, gender) and information about sick leave.

3. Responsible staff for processing data at DVC

Daventry Volunteer Centre Trustee Board is the Data Controller

DVC Manager and project staff are responsible for the data processing

4. The main data risks to DVC

- lost or damaged during a system crash - especially one affecting the hard disk
- corrupted as a result of faulty disks, disk drives, or power failures
- lost by accidentally deleting or overwriting files
- lost or become corrupted by computer viruses
- hacked into by unauthorised users and deleted or altered
- destroyed by natural disasters, acts of terrorism, or war
- deleted or altered by employees wishing to make money or take revenge on their employer

5. **Key precautions to keep data protected and backed up.**

- DVC staff and volunteers will encrypt all confidential info.
- Regular backups will be made of files and the backups stored in another building
- All computers will be password protected and only authorised staff will be allowed to access sensitive data areas.
- Security software will be kept up to date and run on all computers.
- We will not allow unauthorised use of USB storage devices which could lead to data being lost from our organisation.
- The DVC Disaster procedure covers a plan of action to follow if a severe data breach takes place.
- All DVC staff and volunteers will receive training in data protection.
- Where staff or volunteers are using iPads or laptops outside the DVC offices, data will be encrypted.

6. **How the organisation ensures data is kept accurate and when data will be deleted.**

- DVC will ensure that Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- DVC staff will securely delete information that is no longer needed for this purpose or these purposes
- DVC staff will update, archive or securely delete information if it goes out of date.

7. **What to do if an individual asks to see their data.**

Where an individual requests access to data held about them by DVC in writing or verbally, it should be responded to within 1 month of the request. The authenticity of the individual will need to be obtained first.

If an individual informs DVC that the data we hold on them isn't correct, we will take steps to address this as soon as we can practically do so.

8. **Under what circumstances the organisation discloses data, and to whom**

DVC will not share client information with anyone without the individuals consent unless required by law to do so.

Approved by Management Committee 01/06/2018

9. How DVC keeps individuals informed about data it holds.

The DVC staff member responsible for processing data will inform the staff member, volunteer or individuals about the data to be held by DVC at the point of processing.

10.Responsibility for reporting any breaches to the ICO and Charity Commission.

If there is a personal data breach which is defined as:- "a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data." The DVC Manager should be informed immediately, or if not available then the DVC Chair or another DVC Trustee who will decide on what further action is necessary.

If a breach is likely to result in a risk to the rights and freedoms of individuals then the breach must be reported to the ICO (the Information Commissioner's Office) within 72 hours. If a breach is likely to result in a high risk (e.g. criminal activity such as fraud, or published in the public domain) to the rights and freedoms of individuals then those concerned must be notified immediately as failure to notify a breach when there is a requirement to do so can result in a fine. A breach should be reported at www.ico.org.uk/for-organisations/ report-a-breach/

Along with reporting a data breach to the ICO, all charities must report a serious data breach incident to the Charity Commission. The Commission lists the below as a data breach that should be reported:

- Charity's data has been accessed by an unknown person; this data was accessed and deleted, including the charity's email account, donor names and addresses;
- A charity laptop, containing personal details of beneficiaries or staff, has been stolen or gone missing and it's been reported to the police;
- Charity funds lost due to an online or telephone 'phishing scam', where trustees were conned into giving out bank account details;

Agreed by Management Committee 01/06/2018

Next Review date: 01/06/2019