Derbyshire Dales Council for Voluntary Service

Data Protection and Confidentiality Policy

1. Data Protection

Derbyshire Dales Council for Voluntary Service (henceforth **DDCVS**) needs to process certain types of personal data about the data subjects who come into contact with it in order to carry out its work. This personal data must be collected and dealt with appropriately - whether on paper, in a computer, or recorded using other media - and there are safeguards to ensure this personal data under the **EU's General Data Protection Regulation** (henceforth **GDPR**).

DDCVS regards the lawful, fair and transparent treatment of personal data as very important to successful working, and to maintaining the confidence of those with whom we deal. **DDCVS** intends to ensure that personal information is treated lawfully and correctly.

To this end **DDCVS** will adhere to the principles of data protection, as detailed in the **GDPR**.

Specifically, the principles require that personal data is:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) 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;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) 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;

(e) 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;

(f) 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.

Article 5(2) of the GDPF requires that 'the controller shall be responsible for, and be able to demonstrate, compliance with the principles.'

Personal data

This is any information that can directly or indirectly identify a natural person, and can be in any format. Examples of personal data are:

- Name
- Address
- Email address
- Financial details
- Photographs
- IP address
- Location data
- Online behaviour
- Profiling and analytics data

The GDPR refers to sensitive personal data as **special categories of personal data**. Examples of this type of personal data are:

- Race
- Religion
- Political opinions
- Trade union membership
- Sexual orientation
- Health information
- Biometric data
- Genetic data

Data Controller

DDCVS is the Data Controller under the GDPR. The Data Controller determines the purposes and means of processing personal data.

Responsibility

The trustees / directors of **DDCVS** have ultimate responsibility for ensuring **DDCVS**'s compliance with the **GDPR**.

Although it does not necessarily have a statutory obligation to do so, DDCVS will appoint a **Data Protection Officer** (DPO) from the staff team to carry out the following duties:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.

- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, clients, members etc).

DDCVS will ensure that:

- The DPO reports to the highest management level of the organisation (i.e. Board of Trustees).
- The DPO operates independently and will not be dismissed or penalised for performing their task.
- Adequate resources are provided to enable the DPO to meet their GDPR obligations.

Data Subjects

Data subjects of **DDCVS** are likely to include the following:

- Employees and volunteers of DDCVS
- Trustees and Directors of DDCVS
- Members of DDCVS
- Clients of projects and services of DDCVS
- Employees, trustees, directors and volunteers of other organisations with whom we have a working relationship
- People who are interested in the work of DDCVS, and wish to subscribe to our newsletter and attend meetings and events organised by DDCVS

A full analysis of DDCVS' data sets, and how these are processed appears at Annex A.

Data processing

Processing data means obtaining, recording or holding the data or carrying out any operation or set of operations on the data, including:

- organisation, adaptation or alteration of the information or data.
- retrieval, consultation or use of the data.
- disclosure of the data by any means.
- alignment, combination, blocking, erasure or destruction of the data.

Lawful bases for processing

The lawful bases for processing personal data are:

- Direct consent from the individual.
- The necessity to perform a contract.

- Protecting the vital interests of the individual.

- The legal obligations of the organisation.
- Necessity for the public interest.

- The legitimate interests of the organisation.

Most of DDCVS's data processing takes place on the basis of **legitimate interest**. However, there may be other occasions when DDCVS processes data on a basis other than legitimate interest as listed above. On such occasions the data subject will be informed that their data is to be processed on this basis through an appropriate privacy statement.

Where consent is used as a basis for processing, DDCVS will follow these guidelines:

- Consent must be freely given, specific, informed and unambiguous.

- A request for consent must be intelligible and in clear, plain language.

- Consent will not be inferred from silence, pre-ticked boxes and inactivity.

- Consent can be withdrawn at any time.

- DDCVS must be able to evidence consent, even when this is given orally.

Retention of data

DDCVS will retain data for only as long as there is a clear legitimate interest, statutory obligation, or business reason in doing so. We have strict protocols about retention of data. The details of these can be seen at Annex A of this policy.

Data storage, security and safe disposal

DDCVS takes the security of the personal data it processes very seriously, and will take every reasonable measure to ensure against theft or misuse of personal data, and the accidental loss or disclosure of personal data. We aim to ensure this by following these guidelines:

Storage

DDCVS keeps personal data in both electronic and paper formats.

- Electronic personal data is kept primarily in our contacts database. Some personal data is also held our e-mail system Microsoft Outlook within the body of e-mails, or as attachments to e-mails. Other items of personal data may be present in electronic copies of documents stored on our systems (e.g. someone's name and address may appear on a letter, their details may be present on a referral form, or we may have a photograph of them.) Our systems are backed-up daily to a remote server which is housed in a secure alarmed and CCTV monitored location. We use malware and firewall software on all of our systems. Our systems are password protected using

appropriate levels of password complexity and our passwords are changed regularly. Our computer hardware is kept in locked, alarmed locations.

- Paper (‘hard copy’) documents containing personal data are stored in lockable, fire retardant filing cabinets. Keys to the cabinets are kept in a key safe. The office is locked and alarmed at night and weekends, and on other occasions when no staff members are on the premises during normal working hours. Retention of paper documents is kept to a minimum, and would not normally replicate electronic versions of the same document.

Security guidelines for staff

- Keep passwords secure and change regularly as instructed. Do not disclose passwords to anyone without first consulting the Data Protection Officer or a senior manager.
- Passwords must contain at least eight characters, and must contain the following three character classes: alphabetic (e.g. A or a); numeric (e.g. 0-9); punctuation or other characters (e.g. ! or &).
- Lock / log off computers when away from your desk.
- Prevent breaches of cyber security by taking care when opening emails and attachments or visiting new websites.
- Work on a 'clear desk' basis by securely storing hard copy personal data when it is not being used. On no account should personal data be left out on an unattended desk.
- Visitors should be signed in and out of the premises, and accompanied in areas normally restricted to staff.
- Position computer screens away from windows to prevent accidental disclosures of personal data.
- Personal data that is being taken out of the office should be treated with the same level of care as it was still in the office. Think carefully about the need to take personal data off the premises, and how you will keep it secure if you do. This applies to both paper and electronic media.
- Laptops, mobile phones, tablets and external storage devices (such as data sticks) must have been approved by DDCVS. Data sticks will be issued to staff when there is a compelling reason to use one. Data sticks must be returned when the task for which they were issued has been completed.
- Photographs will be taken only with a DDCVS camera that has been issued for the purpose. Photographs should not be taken on mobile phones and other mobile devices. Photographs will be transferred to the DDCVS system as soon as possible, and removed from the camera once this has been done.
- Care should be taken when using diaries and note books to record people’s details. Keep personal data recorded in this way to a minimum, and ensure that diaries and note books a kept securely locked away when not in use. Old diaries and note books containing personal data should be safely destroyed.

Safe disposal

When data is removed from our systems, it will securely disposed of using the following guidelines.

- All personal data kept on paper must be destroyed using DIN 66399 level 3 compliant cross shredder provided by DDCVS.
- Employees are responsible for ensuring that paper-based records that they have taken to the shredder been have properly destroyed. They should not leave papers for shredding unattended at the side of the machine, and ensure that no intact sheets or parts of sheets remain in the shredder, for example due to jamming or power failure.
- General paper waste should be checked carefully before disposal to ensure that it does not contain personal data.
- Where high volumes of paper-based personal data require destruction, DDCVS will arrange to have this professionally destroyed by an organisation with BS EN 15713 certification.
- As far as is practicable, electronic data will permanently deleted from our IT systems so it cannot be viewed or reused.
- Redundant computer hardware will be destroyed professionally. All redundant computer hardware will be destroyed, and will not be sold-on to third parties.

Data access and accuracy

All Data Subjects have the right to access the data **DDCVS** holds about them. **DDCVS** will also take reasonable steps ensure that this data is kept up to date by asking data subjects whether there have been any changes.

In addition, DDCVS will ensure that:

- it has a Data Protection Officer with specific responsibility for ensuring compliance with the General Data Protections Regulation 2018.
- everyone processing personal data understands that they are contractually responsible for following good data protection practice,
- everyone processing personal data is appropriately trained to do so,
- everyone processing personal data is appropriately supervised,
- anybody wanting to make enquiries about handling personal data knows what to do,
- it deals promptly and courteously with any enquiries about handling personal data,
- it describes clearly how it handles personal data,
- it will regularly review and audit the ways it hold, manage and use personal data,
- it regularly assesses and evaluates its methods and performance in relation to handling personal data,
- all staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulation, or any subsequent legislation relating to the processing of personal data.

In case of any queries or questions in relation to this policy please contact the DDCVS Data Protection Officer. This is currently **Sarah Paisley**.

2. Confidentiality

DDCVS is aware of the importance of confidentiality and will ensure that all staff, volunteers and Board members are aware of the confidentiality policy. The confidentiality policy applies to all staff, volunteers and Board members. Any personal or organisational information held by **DDCVS** will remain confidential within DDCVS, and this also applies to any information learned in the course of an individual duties within the organisation.

DDCVS recognises that volunteers, staff members and Board members gain information about individuals and organisations during the course of their work or activities. In most cases this information may not be specifically defined as confidential and individuals may have to exercise common sense and discretion in identifying whether information is expected to be confidential.

Breach of confidentiality

No confidential issue is to be discussed with, or revealed to, any person or organisation outside DDCVS except where the individual or organisation the issue relates to has given express permission. Staff, volunteers and Board members should avoid discussing any confidential issue unless it is relevant to their work.

Staff, volunteers and Board members should avoid exchanging personal information or comments about individuals with whom they have a professional relationship, and they should also avoid talking about organisations or individuals in social settings.

Any member of staff or volunteer found to have breached the confidentiality policy will become subject may be subject to disciplinary action. Any Board member who discloses confidential information or knowledge gained at Board meetings may be asked for their resignation.

Under certain circumstances the organisation has a legal duty, or a duty of care to disclose information. These circumstances include, for example, child protection issues, protection of vulnerable adults, and financial management. If a situation occurs where confidentiality is legally required to be breached, the relevant parties will be informed of action being taken.

Annex A DDCVS summary data set

Data subject	Legal basis	Data gathering	Standard data set	Special category	Format	Disposal
Employees of DDCVS	Legitimate interest	At recruitment, with subsequent additions as appropriate	Name, address, telephone number, e-mail address	Relevant health information	Electronic and paper	Disposed of two years after end of employment. Record of starting and finishing dates retained.
Employees' emergency contacts	Legitimate interest	At recruitment, or subsequently if contact changes	Name and contact number(s)	None	Paper (personnel file)	Disposed of when employee leaves, or contact changes
Directors of DDCVS	Legitimate interest	At the time of registration	Name, address, telephone number, e-mail address	None	Electronic and paper	Disposed of at the end of directorship
Members of DDCVS	Legitimate interest	Membership form	Name, address, telephone number, e-mail address	None	Electronic and paper	When membership ceases, or when the person is no longer the primary contact
Clients of vSPA	Legitimate interest	Referral form, with subsequent additions as appropriate	Name, address, telephone number, e-mail address	Relevant health information	Electronic and paper	Paper records and scans are disposed of 6 months after closure of referral. Anonymised electronic records are held for two years. Copies are held by DVA as the contract manager.
Clients of Escape	Legitimate interest	Referral form, with subsequent additions as appropriate	Name, address, telephone number, e-mail address	Relevant health information	Electronic and paper	Personal data disposed of two years after the last recorded contact from the client
Personnel of other organisations with which we work	Legitimate interest	At point of first contact	Name, address, telephone number, e-mail address	None	Electronic	Personal data disposed of two years after the last recorded contact.
People interested in the work of DDCVS who are not members, and subscribe to the newsletter, attend events etc.	Legitimate interest	At point of first contact	Name, address, telephone number, e-mail address	None	Paper and electronic	Periodic data refreshes identify contacts who no longer wish to have their data retained by DDCVS.

ANNEX B

Handling requests from individuals for their personal data ('data subject access requests')

- People have a right to have a copy of the personal data **DDCVS** holds about them. This is called a 'subject access request'. Such requests must be made in writing, ideally using the standard form provided by DDCVS.
- The organisation has a maximum of 40 days to respond to such a request.
- A fee is not normally charged for such a request.
- Guidelines for dealing with subject access requests are attached at **ANNEX B**

ANNEX C

DDCVS - Subject Access Request Form and Guidance Notes

1. Personal details

Surname:	Former surname (if applicable):	
Mr/Mrs/Ms/Miss:	First name:	
Date of birth:		
Present address:		Postcode:
Phone number:	Mobile number:	

If you have lived at the above address for less than two years (see guidance notes)

Previous address:	Postcode:

2. Details of the information you require

3. Proof of identification - Please list documents/identification supplied *(See note in guidance section)*:

Data Protection Officer, Derbyshire Dales CVS, The Agricultural Business Centre, Agricultural Way, Bakewell DE45 1AH

Signature (of applicant) ……..…… Date …….

Guidance notes for Data Subject Access Requests

Personal details: Please complete your personal details as requested. Please tell us if you have been previously known by any other name and if you have lived at your present address for less than two years, your previous address. If you are requesting historical data then provide as many details as possible; for example, previous addresses with dates. Use a separate sheet of paper if required.

Details of the data you require: You should give as much assistance as you can about particular areas to search so that we can give you what you require without further correspondence. These details are required to assist location of your data so you can be given a copy of everything held about you, as required by the Act.

Proof of identification: Proof of name and address is required to ensure we only give data to the correct person. We require two original pieces of documentation, for example, a recent utility bill, bank statement (photocopies are not acceptable) showing your name *and* address. In some cases additional details such as a passport or photo ID driving licence may be required due to the sensitive nature of data held.

Keep your documents secure: Always send important documents by recorded / special / registered delivery as appropriate. Derbyshire Dales CVS cannot be held liable for items lost in the post.

Payment: A fee is not normally charged for a data access request. However, we may charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive. We may also charge a reasonable fee to comply with requests for further copies of the same information, but not for subsequent access requests. The fee will be based on the administrative cost of providing the information.

Timescale: Any Subject Access Request will be dealt with as quickly as possible. All requests will be dealt with within 40 days of receipt.

If you have any questions relating to identification requirements or any other aspect of a subject access request, you can email us at enquiries@ddcvs.org.uk or call 01629 812154 or write to the Data Protection Officer, Derbyshire Dales CVS, Agricultural Business Centre, Agricultural Way, Bakewell, Derbyshire DE45 1AH

Further information about your rights as a Data Subject can be obtained from the Information Commissioner's Office on **08456 30 60 60** or **01625 54 57 45,** or by visiting the ICO website www.ico.gov.uk