Derbyshire Dales
Council for Voluntary Service

Data Protection and Confidentiality Policy

1.0 Data Protection

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.

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 - UK General Data Protection Act 2018 (UK GDPR) and Data (Use and Access) 2025 (DUA).

DDCVS will adhere to the principles of data protection, as detailed in the **UK GDPR Article 6**.

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 GDPR requires that 'the controller (DDCVS) shall be responsible for, and be able to demonstrate, compliance with the principles.'

2.0 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 UK GDPR Article 9 and DPA 2018 Schedule 1 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

3.0 Data Controller

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

4.0 Responsibility

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

DDCVS will appoint a **Data Protection Officer** (DPO) from the staff team to carry out the following duties as per the UK GDPR Articles 37-39:

- 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 Protection Officer: Shuk-man Woo
Data Protection Officer (Trustee Lead): To be Appointed
Trustee Lead – DPO Officer: Role and Responsibilities – Annex E

5.0 Data Subjects

5.1 Data subjects of **DDCVS** will 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 retention and how these are processed appears at Annex A.

5.2 Data access

All Data Subjects have the right to access the data **DDCVS** holds about them.

The UK GDPR outlines the key rights an individual has concerning their personal data. These rights include:

a) Right to be Informed: Individuals have the right to be informed about the collection and use of their personal data. This includes details about the purposes of processing, retention periods, and who the data will be shared with.
b) Right of Access: Individuals can request access to their personal data and obtain a copy of it. This is often referred to as a Subject Access Request (SAR).
c) Right to Rectification: Individuals have the right to request correction of inaccurate or incomplete personal data.
d) Right to Erasure: Also known as the "right to be forgotten," this allows individuals to request the deletion of their personal data under certain circumstances.
e) Right to Restrict Processing: Individuals can request the restriction of processing their personal data in specific situations, such as when they contest the accuracy of the data.
f) Right to Data Portability: This right allows individuals to obtain and reuse their personal data for their own purposes across different services.

g) Right to Object: Individuals can object to the processing of their personal data in certain circumstances, particularly when the processing is based on legitimate interests or public tasks.
h) Rights Related to Automated Decision-Making and Profiling: Individuals have rights concerning automated decision-making processes, ensuring that significant decisions are not made solely based on automated processing without human intervention.

5.2.1 What is the right of access?
The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data, as well as other supplementary information. It allows individuals to understand how and why you are using their data and check how the DDCVS are doing it lawfully.

5.2.2 How to recognise a subject access request (SAR)?
An individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data. An individual does not need to use a specific form of words, refer to legislation or direct the request to a specific contact.
An individual may ask a third party (eg a relative, friend or solicitor) to make a SAR on their behalf. You may also receive a SAR made on behalf of an individual through an online portal. Before responding, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of their authority.

Upon receipt of a Subject Access Request (SAR), follow the procedure as per Annex B.

5.3 Data Accuracy

DDCVS will take reasonable steps to 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 **Shuk-man Woo.**

Further information about their 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

6.0 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.

6.1 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.

DDCVS's data processing takes place based on **legitimate interest**.

A 'Legitimate Interest Assessment' will be completed by the DPO for all data processing activities and prior to any new or changing of processing activities to confirm that 'legitimate interest' is appropriate for processing data. This document will be reviewed and signed by the Trustee Lead.

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 (Annex D) or direct consent.

Where legitimate interests is used as a basis for processing, a Legitimate Interest Assessment (LIA) will be conducted. Annex C

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.

Any processing of 'Special Categories' as per UK GDPR Article 9, will be based on the following conditions for processing:

(a) Explicit consent
(b) Employment, social security and social protection law
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims and judicial acts
(g) Substantial public interest conditions
(h) Health or social care
(i) Public health
(j) Archiving, research and statistics

For further information: Special category data | ICO

7.0 Data Processing, Sharing and Transfer with Third Parties

DDCVS shares personal data only where necessary for the effective delivery of its day-to-day functions and services.

This may include sharing information with trusted partners, service providers, funders or contractors who support our operational activities. Any such sharing is carried out lawfully, fairly and transparently, and only to the extent required for the specific task or service being delivered.

All third parties receiving data must do so under an appropriate data processing, data sharing agreement or data transfer, ensuring they process the data solely on DDCVS's documented instructions, maintain confidentiality, and implement appropriate security measures in line with UK GDPR Article 28 and 46 requirements.

DDCVS does not transfer data outside the UK or to any country without a UK adequacy decision. Therefore, the UK GDPR rules on international transfers do not apply and the need for a Transfer Risk Assessment is not required but will be reviewed annually.

8.0 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 – Data Retention Schedule of this policy.

9.0 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.

9.1 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.

10.0 Underpinning Policies

Systems and Data Security
Security Incident and Data Breach
Social Media
Cookies

Approved by:				
Date of approval:	May 2026			
Policy version reference:	May 2026			
Policy effective from:	May 2026			
Date for next review:	May 2027			

Annex A – Data Retention Schedule

1. Introduction

DDCVS retains personal data only for as long as there is a clear legal, operational or legitimate interest in doing so. When data is no longer required, it is securely destroyed in line with GDPR principles of storage limitation.

2. General Principles

- Retention periods reflect statutory requirements, funder requirements, and sector best practice.
- Where no statutory timeframe exists, DDCVS applies reasonable retention periods based on operational needs.
- Data is regularly reviewed and securely deleted or anonymised when no longer required.

2.1 Retention Table

Data Category	Examples	Retention Period	Reason
Employee Records	Contracts, HR files, payroll	6 years after employment ends	Limitation Act; HMRC requirements
Volunteer Records	Application, induction, supervision notes	3 years after volunteer leaves	Operational needs; safeguarding
Trustee/Director Records	Contact details, governance documents	6 years after role ends	Charity Commission requirements
Client / Service User Data	Project files, referral info	6 years after case closure (unless project requires otherwise)	Legitimate interest; safeguarding; funder requirements
Safeguarding Records	Concerns, reports, investigations	75 years or as advised by safeguarding authorities	Legal & safeguarding standards
Newsletter Subscribers	Email address, preferences	Until consent withdrawn	Consent-based processing
Event Participants	Registration details	3 years	Legitimate interest; reporting
Financial Data	Invoices, receipts, grant claims	6 years	HMRC requirements
Website Analytics	Cookies, tracking data	Up to 2 years	Industry norms; analytics

2.2 Secure Disposal

Data is disposed of by:

- Cross-shredding paper
- Secure digital erasure

- Confidential-waste services
- Wiping or destroying hardware

Annex B – Subject Access Request (SAR) Procedure

1. Purpose

This annex sets out the procedure for handling requests from individuals exercising their right of access under the UK GDPR.

2. Receiving a SAR

An SAR may be made:
- Verbally
- In writing
- By email or social media
- By a third party authorised to act on someone's behalf

Staff must treat any request for "my data" as a valid SAR.

If you receive an SAR, inform the Data Protection Officer or Chief Executive Officer in case of absence.

Once the DPO has been informed, they will contact the individual concerned and ask them to complete the '**Subject Access Request Form'** and request 'Identity Verification' – Step 3.

3. Identity Verification

DDCVS must be satisfied that the requester is the data subject.
Acceptable ID:
- Two documents showing *name and address* (e.g., utility bill, bank statement)
- For sensitive data: passport or photo driving licence may be required

The 30 day response clock **does not start** until ID is received.

4. Timescales

- Respond **within 30 days** of receiving a complete request.
- You may extend by **up to 60 days** if:
    - the request is complex, or
    - multiple requests are made by the same individual.

The requester must be informed of any extension.

5. Locating the Data

Reasonable steps include:
- Searching emails
- Network folders
- Paper files
- Archived systems
- Project databases

You are *not* required to conduct disproportionate searches.

6. Third-Party Information

If documents contain personal data about someone else:
- Redact the third party's information where possible

- If not possible, seek their consent
- If consent is withheld, assess whether disclosure is reasonable

Always record the decision-making process.

7. Providing the Data

Data should be provided:

- In a **commonly used electronic format** (unless the requester asks otherwise)
- Free of charge (unless manifestly unfounded or excessive)

You should also supply the supplementary information required by Article 15, including:

- Purpose of processing
- Categories of data
- Retention periods
- Rights of rectification/erasure
- The right to complain to the ICO

8. Grounds for Refusal

You may refuse an SAR if:

- It is **manifestly unfounded** or **manifestly excessive**
- An exemption applies (e.g., legal privilege, management forecasting, safeguarding)

The decision to refuse an SAR request must be made jointly by the DPO and the Trustee Lead.

The requester must be told:

- Why the request is refused
- Their right to complain to the ICO
- Their right to seek a court remedy

DDCVS - Subject Access Request Form and Guidance Notes

Derbyshire Dales
Council for Voluntary Service

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 30 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 their 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

Annex C – Legitimate Interest Assessment Guidance and Form

1. Purpose

This annex outlines how DDCVS assesses whether using **Legitimate Interest** is an appropriate lawful basis for processing under Article 6(1)(f) UK GDPR.

2. LIA Structure

A legitimate interest assessment consists of **three tests**:

A. Purpose Test — Is there a legitimate interest?

Examples for DDCVS:

- Delivering charitable services
- Communicating with members and volunteers
- Managing governance and operations
- Securing funding and reporting to funders
- Preventing fraud or safeguarding individuals

Processing is only legitimate if it is lawful, necessary, and ethically justified.

B. Necessity Test — Is processing necessary?

Ask:

- Is the processing proportionate?
- Is there a less intrusive way to achieve the purpose?
- Would failing to process the data cause harm or inefficiency?

If the purpose cannot reasonably be achieved otherwise, processing is considered necessary.

C. Balancing Test — Do the individual's rights override the interest?

Consider:

- Nature and sensitivity of the data
- Reasonable expectations of the data subject
- Impact on individuals (positive or negative)
- Safeguards in place (minimal data; secure storage; right to object)

If risks outweigh benefits, legitimate interest cannot be used.

3. LIA Outcomes

The assessment may conclude:

- **Legitimate interest applies**
- **Legitimate interest applies with additional safeguards**
- **Legitimate interest does not apply** (choose another lawful basis)

A written record of each assessment must be retained.

4. Transparency

Where legitimate interest is used, DDCVS must:

- Explain this in the relevant **privacy statement**
- Inform individuals of their **right to object**

5. Annual Review

All LIAs are reviewed annually or whenever:

- New processing activities begin
- Services or technologies change
- Risks to individuals change

Legitimate Interest Assessment – Template

This legitimate interests assessment (LIA) template is designed to help you to decide whether or not the legitimate interests basis is likely to apply to your processing. It should be used alongside our legitimate interests guidance.

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

- Why do you want to process the data?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are the benefits that you have identified?
- What would the impact be if you couldn't go ahead with the processing?
- Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice?
- Are there any other ethical issues with the processing?

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

- Will this processing actually help you achieve your purpose?
- Is the processing proportionate to that purpose?
- Can you achieve the same purpose without the processing?

- Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

Nature of the personal data

- Is it special category data or criminal offence data?
- Is it data which people are likely to consider particularly 'private'?
- Are you processing children's data or data relating to other vulnerable people?
- Is the data about people in their personal or professional capacity?

Reasonable expectations

- Do you have an existing relationship with the individual?
- What's the nature of the relationship and how have you used data in the past?
- Did you collect the data directly from the individual? What did you tell them at the time?
- If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
- How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
- Is your intended purpose and method widely understood?
- Are you intending to do anything new or innovative?
- Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation?
- Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

Likely impact

- What are the possible impacts of the processing on people?
- Will individuals lose any control over the use of their personal data?
- What is the likelihood and severity of any potential impact?
- Are some people likely to object to the processing or find it intrusive?
- Would you be happy to explain the processing to individuals?
- Can you adopt any safeguards to minimise the impact?

Can you offer individuals an opt-out?	Yes / No

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

Can you rely on legitimate interests for this processing?	Yes / No
Do you have any comments to justify your answer? (optional)	
LIA completed by	
Date	
Reviewed by Trustee Lead	
Date	

What's next?

Keep a record of this LIA, and keep it under review.

Do a DPIA if necessary.

Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.

Annex D - DDCVS Privacy Notice

We collect and retain only the minimum amount of data need to enable us to service your membership of DDCVS, or your interaction with DDCVS. Your data will be kept in both electronic and paper formats. We make every effort to ensure that your data is secure, and that it is kept up to date.

We will retain your data only for as long as your membership of DDCVS lasts or for as long as your interaction with DDCVS continues. If your organisation withdraws from membership, or you are no longer the primary contact for your organisation, then your data will be fully deleted from our systems, and any paper records will be safely disposed of.

A Transfer Risk Assessment is not required because no personal data is transferred outside the UK or to any country without a UK adequacy decision. The UK GDPR rules on international transfers therefore do not apply.

We do not sell data to any organisation.

You have many rights regarding your personal data, including seeing the data we collect and store, and updating your information. We use our website hosted by Website Design Derby and a web-based CRM software called Aide to send out our newsletter: you are able to unsubscribe at any time by using the 'unsubscribe' link or by emailing enquiries@ddcvs.org.uk

Annex E

Trustee Lead – DPO Officer: Role and Responsibilities