DERBYSHIRE CAVING CLUB

Data protection policy

Key details

- Policy prepared by: Nigel Dibben (Webmaster and Hon. Treasurer)
- Approved by committee on: TBA.
- Policy became operational on: TBA.
- Next review date: One year.

Introduction

Derbyshire Caving Club (DCC) needs to gather and use certain personal information about individuals.

These individuals can include members, prospective members, Alderley Mine visitors on routine trips, Alderley Mine visitors on open days and other people the organisation has a relationship with or may need to contact (e.g. annual dinner guests).

This policy describes how this personal data must be collected, handled and stored to meet the Club's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures Derbyshire Caving Club:

- Complies with data protection law and follows good practice
- Protects the rights of members, visitors and others
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 2018 and the UK General Data Protection Regulation describe how organisations — including Derbyshire Caving Club — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act 2018 is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Policy scope

This policy applies to:

- The officers of the DCC (i.e. the Chairman, Hon. Secretary and Hon. Treasurer)
- The members of the DCC
- Contractors, suppliers and other people working on behalf of the DCC

It applies to all data that the Club holds relating to identifiable individuals, even if that information technically falls outside of the Regulations. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Year of birth
- Car registration
- Emergency contacts
- BCA membership details
- plus any other information relating to identifiable individuals

Lawful basis for processing personal data

The DCC processes data for the following reasons:

- To maintain records of membership including: maintaining an up-to-date list of members' names for all members to see; requesting and processing subscriptions; enabling communication to members by post, email or telephone.
- To manage applications for membership including disclosing the names of potential members to the existing membership.
- To insure members through the BCA insurance scheme.
- To reserve places at Alderley Edge Open Days and on other trips for the general public and to communicate with those who have reserved places before the day and on the day.
- To obtain and retain lists of visitors to the Alderley Edge Mines as required by the Club's Public Liability insurer.
- To enable members to be named on photographs, within on-line reports of activities and in newsletters produced by the Club.

- To manage bookings for the Annual Club Dinner and any similar events where names and contact details together with dietary preferences are collected, stored and may be reproduced on documentation for the event.

Data protection risks

This policy helps to protect the DCC from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the Club uses data relating to them.
- **Reputational damage.** For instance, the Club could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone member of the DCC has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Officers** are ultimately responsible for ensuring that the DCC meets its legal obligations.
- The **Hon. Secretary** is responsible for:

  Keeping the Officers and Committee updated about data protection responsibilities, risks and issues.
  Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  Arranging data protection training and advice for the people covered by this policy.
  Handling data protection questions from members and anyone else covered by this policy.
  Dealing with requests from individuals to see the data that the DCC holds about them (also called 'subject access requests').
  Checking and approving any contracts or agreements with third parties that may handle the DCC's sensitive data.
  Approving any data protection statements attached to communications such as emails and letters.
  Addressing any data protection queries from journalists or media outlets like newspapers.

- The **Webmaster** is responsible for:

  Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  Performing regular checks and scans to ensure security hardware and software is functioning properly.

Evaluating any third-party services the DCC is considering using to store or process data. For instance, cloud computing services.

General guidelines for members

- The only people able to access data covered by this policy should be those who **need it for their responsibility within the Club**. This would include, for example, leading trips into the Alderley Mines, handling membership enquiries, and mailing newsletters.
- Data **should not be shared informally**. When access to confidential information is required, members can request it from the Hon. Secretary, Membership Secretary or Webmaster.
- As and when appropriate, **the DCC will provide training** to members to help them understand their responsibilities when handling data.
- Members should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the DCC or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Members **should request help** from the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely on paper can be directed to the Hon. Secretary and on-line to the Webmaster.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When data is stored on paper such as membership forms:

  When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
  Specifically, completed lists of Alderley visitors should be posted after the trip into **the locked container** provided in the Surgery.
  Members should make sure paper and printouts are **not left where unauthorised people could see them**, such as on a printer.
  Data printouts should be shredded and disposed of securely when no longer required.

- When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

Data should be **protected by strong passwords** that are changed regularly and never shared between members.

If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.

Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.

Data should be **backed up frequently**. Those backups should be tested regularly, in line with the Club's standard backup procedures.

Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones without adequate password protection and/or encryption.

All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

It is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, misuse or theft:

- When working with personal data in a public place, members should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure. The Webmaster can show members how to transfer data securely.
- Data must be **encrypted before being transferred electronically**. The Webmaster can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the UK.

Data accuracy

The law requires the DCC to take reasonable steps to ensure data is kept accurate and up to date. It is most important that the personal data is accurate, and greater effort should be put into ensuring its accuracy. It is the responsibility of all members who use personal data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Members should not create any unnecessary additional data sets.
- Members and the officers should **take every opportunity to ensure data is updated.** For instance, by confirming a member's details periodically.
- The DCC will make it **easy for data subjects to update the information** that the Club holds about them, for instance, via the Club website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a member can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by the DCC are entitled to:

- Ask **what information** the Club holds about them and why.

- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the Club is meeting its data protection obligations.

If an individual contacts the Club requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data controller at **secretary@derbyscc.org.uk**. The data controller can supply a standard request form, although individuals do not have to use this. Individuals will not be charged for a subject access request. The data controller will aim to provide the relevant data within 14 days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act/GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, the DCC will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the other officers and from the Club's legal advisers where necessary.

Providing information

The DCC aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the Club has a privacy statement, setting out how data relating to individuals is used by the Club.

This is available on request. A version of this statement is also available on the Club's website.

Draft

Updated: 12 April, 2022

Author: Nigel Dibben, Webmaster