



Hereford Lads Club

Data Protection Policy

Purpose:

Hereford Lads Club is committed to protecting the privacy and security of personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy outlines how the club collects, processes, stores, and protects personal data, ensuring the rights and privacy of all individuals are upheld.

Scope:

This policy applies to:

- Hereford Lads Club
- All staff, volunteers, parents of Hereford Lads Club

This policy applies to all personal data processed by Hereford Lads Club, including data relating to members, players, parents, guardians, staff, volunteers, and any other individuals associated with the club.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus any other information relating to individuals

Data protection law

The Data Protection Act 1998 describes how organisations — including HLC — 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 is underpinned by eight important principles.

These say that personal data must:

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

People, Risks and Responsibilities

Data protection risks

This policy helps to protect HLC 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 company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

In the event of a data breach, the club will:

- Investigate the breach immediately.
- Take steps to mitigate any potential harm.
- Depending on the severity of the breach disciplinary action may be taken in line with HLC Code of Conduct and the Welfare and Disciplinary process.
- Notify the ICO and affected individuals, if required, in accordance with legal obligations.

Any suspected or actual breach must be reported to the Data Protection Officer or Club Welfare Officers. Swift reporting ensures appropriate action can be taken to minimise harm and comply with legal obligations.

Responsibilities

- Data Controller: Hereford Lads Club is the Data Controller responsible for determining the purposes and means of processing personal data.
- Data Protection Officer (DPO): The club's appointed DPO oversees compliance with data protection laws, provides guidance, and addresses queries related to this policy.
- Committee Members, Volunteers and Parents: All individuals handling personal data must comply with this policy.

These people have key areas of responsibility:

• The Chairman Chris Price is ultimately responsible for ensuring that HLC meets its legal obligations and is responsible for:

- Keeping volunteers 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 advice for the people covered by this policy.
- Handling data protection questions from volunteers and anyone else covered by this policy.
- Dealing with requests from individuals to see the data HLC holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- 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 company is considering using to store or process data. For instance, cloud computing services.
- 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.
- Where necessary, working with other volunteers to ensure any initiatives abide by data protection principles.

Committee Members, Volunteers and Parents

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, it can be requested from the Chairman
- All data should be kept secure, by taking sensible precautions and following the guidelines below.
- Personal data **should not be disclosed** to unauthorised people.
- 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.
- Any data that forms part of a **disciplinary process must not be disclosed** to unauthorised people.
- Help from the Chairman should be obtained if they are unsure about any aspect of data protection.

Collection and Use of Data

Hereford Lads Club collects personal data such as names, contact information, health details (for safeguarding purposes), and emergency contact details. The data is used for:

- Managing club membership and participation.
- Safeguarding and welfare purposes.
- Communication with members, parents, and guardians.
- Compliance with legal and regulatory requirements

Data accuracy

The law requires HLC to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort HLC should put into ensuring its accuracy.

It is the responsibility of all employees who work with 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.
- Volunteers should take every opportunity to ensure data is updated.
- Data should be updated as inaccuracies are discovered.

Data Storage

These rules describe how and where data should be safely stored.

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 not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Volunteers should make sure paper and printouts are **not left where unauthorised people could see them**.
- **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 employees.
- 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**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.
- Personal data will be **retained only for as long as necessary** for the purpose for which it was collected. Once no longer needed, data will be securely deleted or anonymized.

Disclosing data for other reasons

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

Under these circumstances, HLC will disclose requested data. However, HLC will ensure the request is legitimate, seeking assistance from the local FA.

Rights of Individuals

Individuals have the following rights under data protection laws:

- Access: The right to access their personal data and obtain information about how it is processed.
- Rectification: The right to have inaccurate or incomplete data corrected.
- Erasure: The right to request the deletion of personal data in certain circumstances.
- Restriction: The right to restrict processing of personal data in specific situations.
- Portability: The right to receive their data in a structured, commonly used, and machine-readable format.
- Objection: The right to object to processing based on legitimate interests or direct marketing.
- Complaints: The right to lodge a complaint with the Information Commissioner's Office (ICO).

Subject Access Requests

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

- Ask **what information** the organisation 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 company is **meeting its data protection obligations**.

If an individual contacts the organisation requesting this information, this is called a subject access request.

Subject access requests

Subject access requests from individuals should be made by email, addressed to the Chairman.

HLC will aim to provide the relevant data within 28 days.

HLC will always verify the identity of anyone making a subject access request before handing over any information.

Review and Updates:

This policy will be reviewed annually or as required to reflect changes in data protection laws, guidance, or club practices.

By adhering to this policy, Hereford Lads Club ensures the privacy and trust of all individuals associated with the club are respected and protected.

Chris Price- Chairman- chairman.herefordladsclub@gmail.com

Oliver Williams- Data Protection Officer/ Vice Chairman- vicechairman.herefordladsclub@gmail.com

Katrina Williams- Lead Welfare Officer- welfare.herefordladsclub@gmail.com

HLC Lead CWO: Katrina Williams
Email: welfare.herefordladsclub@gmail.com
Data Protection Policy 2025/2026