UNITY SPORTS COLLECTIVE CIC

DATA PROTECTION & GDPR POLICY

1. Purpose of this Policy

USC is committed to protecting the personal information of children, young people, parents, carers, staff, volunteers, coaches, partners, supporters and members of the community.

This policy explains how USC will collect, use, store, share and dispose of personal information in a lawful, fair, transparent and secure way. It also explains how USC will meet its responsibilities under UK data protection law, including the UK General Data Protection Regulation, the Data Protection Act 2018 and any relevant updates to data protection legislation.

USC recognises that it may hold sensitive information about children, young people and families. This means the organisation must take particular care to protect privacy, confidentiality and safety.

2. Scope of this Policy

This policy applies to all personal data processed by USC, whether held electronically, on paper, in photographs, on video, in emails, on forms, in databases, on phones, on cloud storage, through messaging platforms, or in any other format.

This includes information relating to:

- children and young people attending USC activities;
- parents, carers and emergency contacts;
- staff, volunteers, coaches and trustees/directors;
- partner organisations and professionals;
- donors, funders, supporters and community members;
- safeguarding, health, accident, incident and consent records;
- photographs, videos and promotional material;
- attendance registers, registration forms and monitoring information.

Everyone working with or on behalf of USC must follow this policy.

3. Key Definitions

Personal data means any information that can identify a living person. This may include a name, address, phone number, email address, date of birth, photograph, video, ID number, online identifier, or information about a person's circumstances.

Special category data means more sensitive personal information, such as information about health, ethnicity, religion, disability, biometric data, or other protected information.

Data subject means the person the information is about.

Processing means anything USC does with personal data, including collecting, recording, storing, using, sharing, deleting or destroying it.

Data controller means the organisation that decides why and how personal data is used. USC will usually be the data controller for the information it collects and uses for its own activities.

Data processor means another organisation or person that processes personal data on USC's behalf, such as a cloud storage provider, email platform, booking system or payroll provider.

Personal data breach means a security incident that leads to personal data being lost, accessed, disclosed, altered, destroyed or shared without proper authority.

4. Data Protection Principles

USC will follow the seven main data protection principles. Personal data must be:

1. **Processed lawfully, fairly and transparently** – USC will only use personal data where it has a valid reason and will be clear with people about how their information is used.
2. **Collected for specified, explicit and legitimate purposes** – USC will only collect information for clear reasons connected to its activities and responsibilities.
3. **Adequate, relevant and limited to what is necessary** – USC will only collect the information it genuinely needs.
4. **Accurate and kept up to date** – USC will take reasonable steps to keep records accurate.
5. **Kept only for as long as necessary** – USC will not keep personal data longer than needed.
6. **Handled securely** – USC will protect personal data from unauthorised access, loss, damage, misuse or disclosure.
7. **Handled with accountability** – USC will be able to demonstrate that it takes data protection seriously and has appropriate measures in place.

5. Types of Information USC May Collect

USC may collect and process the following types of personal information:

5.1 Children and young people

- name;
- date of birth and age;
- address or general location, where needed;

- parent/carer contact details;
- emergency contact details;
- medical information relevant to participation;
- allergy information;
- disability or access needs;
- attendance records;
- consent forms;
- safeguarding concerns, where relevant;
- accident and incident records;
- photographs or videos, where consent has been given;
- monitoring information required by funders, where appropriate.

5.2 Parents and carers

- name;
- contact details;
- relationship to the child or young person;
- emergency contact information;
- consent information;
- communication records.

5.3 Staff, volunteers, coaches and directors

- name and contact details;
- role and availability;
- recruitment information;
- references;
- DBS information, where appropriate;
- training records;
- safeguarding records;
- payment or bank details, where relevant;
- emergency contact details;
- equality and diversity monitoring information, where collected.

5.4 Community members, supporters, partners and funders

- name;
- organisation;
- contact details;
- communication records;
- donation or funding information;
- attendance at USC events or activities.

6. Why USC Collects and Uses Personal Data

USC may collect and use personal data for the following purposes:

- to register children and young people for activities;
- to manage attendance and participation;

- to keep children and young people safe;
- to contact parents, carers or emergency contacts;
- to assess suitability for activities and identify support needs;
- to respond to accidents, incidents or medical needs;
- to meet safeguarding responsibilities;
- to recruit, support and manage staff, coaches and volunteers;
- to comply with legal, insurance, funding and governance requirements;
- to evidence project delivery and impact;
- to communicate about activities, events and opportunities;
- to promote USC's work, where appropriate consent has been obtained;
- to respond to complaints, concerns or requests;
- to manage partnerships and professional referrals.

7. Lawful Basis for Processing Personal Data

USC will identify a lawful basis before processing personal data. The lawful basis may vary depending on the purpose.

USC may rely on one or more of the following lawful bases:

7.1 Consent

USC may rely on consent where a person has clearly agreed to their information being used for a specific purpose. This may include consent for photographs, videos, publicity, newsletters or optional communication.

Where consent is used, individuals have the right to withdraw consent at any time.

For children and young people, USC will usually seek consent from a parent or carer, unless the young person is considered able to understand and make the decision themselves.

7.2 Contract

USC may process personal data where it is necessary to fulfil an agreement, such as employment, volunteering, coaching, service delivery or paid activity arrangements.

7.3 Legal obligation

USC may process personal data where required by law, such as for safeguarding, employment, tax, health and safety, insurance, accounting or reporting obligations.

7.4 Vital interests

USC may process or share personal data where necessary to protect someone's life or respond to a serious emergency, such as a medical incident.

7.5 Legitimate interests

USC may process personal data where it has a legitimate reason to do so and where this does not override the rights, freedoms or interests of the individual. This may include basic administration, communication with families, volunteer coordination, project management, organisational record keeping, impact reporting and protecting USC's interests.

Where USC relies on legitimate interests, it will consider whether the processing is necessary, proportionate and reasonable.

8. Special Category Data

USC may sometimes need to collect special category data, such as health information, disability information, allergy details, ethnicity or other sensitive information. This will only be collected where necessary and where there is a clear lawful reason.

USC may collect this information to:

- keep children, young people, staff and volunteers safe;
- make reasonable adjustments;
- respond to medical needs;
- meet safeguarding responsibilities;
- monitor equality, diversity and inclusion;
- meet funder reporting requirements, where appropriate.

Special category data will be handled with additional care and only shared with people who need to know.

9. Children and Young People's Information

USC recognises that children and young people's personal data requires particular protection.

USC will:

- only collect information that is necessary for safe and effective delivery;
- ensure parents and carers understand what information is collected and why;
- explain privacy information in a clear and age-appropriate way where possible;
- avoid collecting unnecessary sensitive information;
- keep children's information secure;
- restrict access to children's records to authorised people only;
- never share children's personal information casually or unnecessarily;
- ensure photographs and videos are only used in line with USC's consent procedures and safeguarding practice.

10. Photographs, Videos and Publicity

USC may use photographs or videos to celebrate activities, promote its work, report to funders, or share positive community stories. However, USC recognises that images of children and young people must be managed carefully.

USC will:

- obtain written consent before using identifiable photographs or videos for publicity;
- explain where images may be used, such as social media, websites, newsletters, reports or flyers;
- avoid using full names alongside children's photographs unless there is a clear reason and specific consent;
- respect any refusal or withdrawal of consent;
- avoid sharing images that may embarrass, exploit or place a child or young person at risk;
- store images securely;
- remove images where reasonably possible if consent is withdrawn.

Staff, volunteers, coaches and visitors must not take or share photographs or videos of children or young people for personal use.

11. Privacy Notices

USC will provide clear privacy information to individuals at the point where personal data is collected, or as soon as reasonably possible afterwards.

A privacy notice should explain:

- what information USC collects;
- why USC collects it;
- USC's lawful basis for using it;
- who the information may be shared with;
- how long USC will keep it;
- the individual's rights;
- how to contact USC about data protection concerns.

USC may use separate privacy notices for children and families, staff, volunteers, supporters or website users where appropriate.

12. Data Sharing

USC will not sell personal data.

USC will only share personal data where there is a valid reason to do so. This may include sharing information with:

- parents or carers;

- emergency services;
- safeguarding agencies;
- local authorities;
- schools or youth services, where appropriate;
- funders, where reporting is required and lawful;
- insurers;
- accountants or payroll providers;
- IT, email, cloud storage or booking system providers;
- professional advisers;
- regulatory bodies, where required.

Where possible, USC will share anonymised or aggregated information instead of identifiable personal data.

USC may share personal data without consent where required by law, where there is a safeguarding concern, where someone is at risk of harm, or where it is necessary to protect someone's vital interests.

13. Safeguarding and Confidentiality

Data protection law does not prevent USC from sharing information where it is necessary to safeguard a child, young person or adult at risk.

Where there is a safeguarding concern, USC will share relevant information with the Designated Safeguarding Lead, statutory agencies, police, local authority children's services, adult safeguarding services, or other appropriate professionals.

Only relevant and necessary information will be shared, and a clear record will be kept of what was shared, with whom, when and why.

Confidentiality must never be promised where there is a risk of harm or where USC has a legal or safeguarding duty to act.

14. Data Security

USC will take reasonable steps to keep personal data secure.

This may include:

- using password protection on devices and accounts;
- using strong passwords and, where possible, two-factor authentication;
- limiting access to personal data to those who need it for their role;
- storing paper records in locked cabinets or secure locations;
- avoiding unnecessary printing of personal data;
- keeping registers, forms and records out of public view;
- using secure email and cloud storage systems;
- avoiding the use of personal devices where possible;
- ensuring personal data is not left unattended at sessions or events;

- securely deleting or shredding personal data when no longer needed;
- reporting any suspected breach immediately.

Staff, volunteers and coaches must not share personal data through informal channels unless it is necessary, secure and authorised.

15. Use of WhatsApp, Email and Messaging Platforms

USC may use email, phone calls, texts or messaging platforms to communicate with parents, carers, volunteers and partners.

When using messaging platforms, USC will:

- avoid sharing sensitive personal data unless necessary;
- avoid posting children's personal information in group chats;
- use broadcast lists or direct messages where this better protects privacy;
- ensure group members understand the expected standards of behaviour and confidentiality;
- remove people from groups when they no longer need access;
- avoid sharing safeguarding details in general group chats;
- keep professional boundaries when communicating with children, young people and families.

Any communication involving safeguarding concerns must be handled in line with USC's Safeguarding Policy.

16. Paper Records

Paper records must be kept secure at all times. This includes registration forms, consent forms, accident records, incident records, safeguarding notes and attendance registers.

USC will:

- store paper records securely;
- limit access to authorised people;
- avoid leaving forms visible during sessions;
- transport records securely when needed;
- shred confidential records when they are no longer required.

17. Electronic Records

Electronic records must be stored securely using appropriate systems.

USC will:

- use password-protected systems;
- restrict access to authorised users;
- avoid saving confidential records on unsecured personal devices;

- ensure cloud storage folders are not open to unauthorised users;
- regularly review shared access permissions;
- delete records securely when no longer needed;
- back up important records where appropriate.

18. Data Retention

USC will not keep personal data for longer than necessary. Retention periods will depend on the type of record, the reason it was collected and any legal, safeguarding, insurance or funder requirements.

USC will review records regularly and securely delete or destroy information that is no longer needed.

Suggested retention periods are set out below. USC should adapt these where required by law, funder conditions, insurance requirements or safeguarding advice.

Type of record	Suggested retention period
General activity registration forms	Up to 3 years after last attendance
Attendance registers	Up to 3 years after the activity or funding period ends
Parent/carer contact details	Until no longer needed, then securely deleted
Photo/video consent forms	For as long as the image is used, then reviewed
Accident records involving children	Until the child reaches age 21, or longer if required by insurance
Serious incident records	At least 6 years, or longer where appropriate
Safeguarding records	In line with safeguarding guidance and statutory requirements; usually retained securely for a longer period
Volunteer records	Up to 6 years after leaving, depending on the record type
Staff records	Up to 6 years after employment ends, unless a longer period is required
DBS certificate information	USC should not keep copies longer than necessary; record check details securely only where appropriate
Financial records	Usually 6 years
Complaints records	Usually 6 years after closure, depending on seriousness
Funder monitoring records	In line with funder agreement, usually 3–6 years

Where records relate to safeguarding, legal claims, complaints, accidents or serious incidents, USC may need to keep them for longer.

19. Individual Rights

Individuals have rights under data protection law. These may include the right to:

- be informed about how their data is used;
- access their personal data;
- ask for inaccurate data to be corrected;
- ask for data to be erased in certain circumstances;
- restrict how data is used in certain circumstances;
- object to certain types of processing;
- ask for data portability in certain circumstances;
- not be subject to certain automated decision-making.

Requests should be sent to: **unitysccic@outlook.com**

USC will respond to rights requests within the required legal timeframe, normally one month. USC may need to confirm the person's identity before responding.

Some rights are not absolute. For example, USC may need to keep certain records for safeguarding, legal, insurance or regulatory reasons.

20. Subject Access Requests

A subject access request is a request from an individual to see the personal data USC holds about them.

If USC receives a subject access request, the request must be passed to the policy owner or relevant senior person immediately.

USC will:

- acknowledge the request;
- verify the person's identity where necessary;
- locate relevant records;
- consider whether any exemptions apply;
- protect third-party information;
- respond within the required legal timeframe.

Staff, volunteers and coaches must not ignore or delay passing on a request.

21. Personal Data Breaches

A personal data breach may include:

- losing a paper form or register;
- sending an email to the wrong person;
- sharing a document with the wrong person;
- losing a phone, laptop or USB stick containing personal data;

- unauthorised access to a database or email account;
- accidental disclosure of safeguarding or medical information;
- posting a photograph without consent;
- a cyber-attack or hacking incident.

All suspected or actual breaches must be reported immediately to **[Insert name/role]**.

USC will:

- record the breach;
- assess what happened;
- identify what data was involved;
- consider who may be affected;
- take steps to reduce harm;
- decide whether the breach must be reported to the Information Commissioner's Office;
- decide whether affected individuals must be informed;
- review procedures to prevent the breach happening again.

Where a breach is likely to result in a risk to people's rights and freedoms, USC may need to report it to the Information Commissioner's Office within 72 hours of becoming aware of it.

22. Data Processors and Third-Party Systems

Where USC uses third-party systems or service providers to process personal data, USC will take reasonable steps to ensure they provide appropriate data protection safeguards.

This may include checking:

- how the provider stores and protects data;
- whether access is password protected;
- whether data is stored in the UK, EEA or another country;
- whether there are appropriate contractual terms;
- whether data can be deleted when no longer needed;
- whether the provider has appropriate security standards.

Examples may include email providers, cloud storage, booking systems, payroll providers, website platforms, online forms and accountancy software.

23. International Transfers

USC will take care when using systems that may store or process data outside the UK. Where personal data is transferred outside the UK, USC will ensure there are appropriate safeguards in place, where required by data protection law.

24. Training and Awareness

USC will ensure that staff, volunteers, coaches and directors understand their data protection responsibilities.

This may include:

- induction information;
- safeguarding and confidentiality training;
- guidance on safe communication;
- reminders about secure record keeping;
- updates when procedures change.

Everyone involved in USC must understand that personal data must only be accessed or shared where there is a valid reason.

25. Roles and Responsibilities

Directors/management committee

The directors or management committee are responsible for ensuring that USC has appropriate data protection arrangements in place.

Policy owner

The policy owner is responsible for overseeing this policy, supporting compliance, managing data protection concerns and coordinating responses to breaches or rights requests.

Staff, coaches and volunteers

All staff, coaches and volunteers are responsible for:

- following this policy;
- keeping personal data confidential;
- only collecting information that is needed;
- keeping records secure;
- reporting breaches immediately;
- asking for advice if unsure.

Designated Safeguarding Lead

The Designated Safeguarding Lead is responsible for ensuring that safeguarding information is handled securely, shared appropriately and recorded properly.

26. Confidentiality

Everyone working with or on behalf of USC must keep personal information confidential.

Personal information must not be discussed in public places, shared with friends or family, posted online, or accessed out of curiosity.

Confidentiality may be overridden where there is a safeguarding concern, legal duty, serious risk of harm, or other valid reason for sharing information.

27. Monitoring and Review

This policy will be reviewed at least annually, or earlier if:

- there are changes in data protection law or guidance;
- USC changes how it collects or uses personal data;
- there is a personal data breach;
- there are changes to USC's activities, systems or structure;
- a funder, regulator or partner requires updates.

USC will keep this policy under review to ensure it remains practical, lawful and appropriate for the organisation.

28. Related Policies and Documents

This policy should be read alongside:

- Safeguarding Children Policy;
- Safeguarding Adults Policy, if applicable;
- Health and Safety Policy;
- Risk Assessment Procedure;
- Equality, Diversity and Inclusion Policy;
- Volunteer Policy;
- Complaints Policy;
- Privacy Notices;
- Consent Forms;
- Photo and Video Consent Form;
- Data Retention Schedule;
- Incident and Accident Reporting Forms.

14. Adoption of Policy

Carlos Lerma
Founder/Director
Unity Sports Collective (USC)

Adopted on:	June 2025
Review on:	June 2026