DATA PROTECTION POLICY

1. Introduction

Cambridge United Football Club (CUFC) needs to collect and use certain types of information about the Individuals or Service Users who we come into contact with in order to carry on our work. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the EU General Data Protection Regulation 2018.

Data protection is important to CUFC so that the organization can comply with relevant legislation, to ensure we offer the best possible service to those we interact with and also to ensure safety for all staff and participants.

2. Data Controller

CUFC is the Data Controller under the Regulation, which means that it determines what purposes personal information will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

3. Disclosure

CUFC may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Individual/Service User will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows CUFC to disclose data (including sensitive data) without the data subject's consent.

These are:

- Carrying out a legal duty or as authorised by the Secretary of State
- Protecting vital interests of a Individual/Service User or other person
- The Individual/Service User has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes – i.e. race, disability or religion
- Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures.

CUFC regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

CUFC intends to ensure that personal information is treated lawfully and correctly.

To this end, CUFC will adhere to the Principles of Data Protection, as detailed in the EU General Data Protection Regulation 2018.

Specifically, the Principles require that personal information:

- Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met,
- Shall be obtained only for one or more of the purposes specified in the Regulation, and shall not be processed in any manner incompatible with that purpose or those purposes,
- Shall be adequate, relevant and not excessive in relation to those purpose(s)
- Shall be accurate and, where necessary, kept up to date,
- Shall not be kept for longer than is necessary
- Shall be processed in accordance with the rights of data subjects under the Regulation,
- Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
- Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals/Service Users in relation to the processing of personal information.

CUFC will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the rights of people about whom information is held, can be fully exercised under the Regulation. These include:
    - The right to be informed that processing is being undertaken,
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information
- Take appropriate technical and organisational security measures to safeguard personal information, including taking reasonable measures to ensure the physical security of such equipment that may be used to store/access personal information
- Ensure that personal information is not transferred abroad without suitable safeguards

- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

4. Data collection

Informed consent is when an Individual/Service User clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data, and then gives their consent.

CUFC will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data, CUFC will ensure that the Individual/Service User:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

Staff/volunteers who are asked to collect data on behalf of CUFC will be reminded of their responsibilities and will report any issues regarding these responsibilities to the Data Protection Officer.

5. Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.

Access is managed via password-protected secure folders which access only available to staff who have a need to access the data.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is CUFC's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

Staff/volunteers of CUFC will not store information or records relating to service users on shared computers/laptops, and agree that all data held on personal laptops/computers is held there for the minimum possible time, and is made non-recoverable as soon as this period has elapsed.

Physical access to any printed personal data is controlled by being kept in secure locations and documents being shredded as soon as the need to have them in physical form expires. The office in which the documents are hosted is also locked and access to the building is closely monitored.

Password Policy

Employees at CUFC must access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. Passwords are a key part of the strategy to make sure only authorized people can access those resources and data.

All employees who have access to any of those resources are responsible for choosing strong passwords and protecting their log-in information from unauthorized people.

The purpose of this policy is to make sure all CUFC resources and data receive adequate password protection. The policy covers all employees who are responsible for one or more account or have access to any resource that requires a password.

Password creation

All passwords should be reasonably complex and difficult for unauthorized people to guess. Employees should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. These requirements will be enforced with software when possible.

In addition to meeting those requirements, employees should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" are equally bad from a security perspective.

A password should be unique, with meaning only to the employee who chooses it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase "This may be one way to remember" can become "TmB0WTr!".

Employees must choose unique passwords for all of their company accounts, and may not use a password that they are already using for a personal account.

All passwords must be changed regularly, with the frequency varying based on the sensitivity of the account in question.

If the security of a password is in doubt– for example, if it appears that an unauthorized person has logged in to the account — the password must be changed immediately.

Default passwords — such as those created for new employees when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.

Protecting passwords

Employees may never share their passwords with anyone else, including colleagues. Everyone who needs access to a system will be given their own unique password.

Employees may never share their passwords with any outside parties, including those claiming to be representatives of a business partner with a legitimate need to access a system.

Employees should take steps to avoid phishing scams and other attempts by hackers to steal passwords and other sensitive information.

Employees must refrain from writing passwords down and keeping them at their workstations. See above for advice on creating memorable but secure passwords.

Employees may not use password managers or other tools to help store and remember passwords without permission.

6. Data access and accuracy

All Individuals/Service Users have the right to access the information CUFC holds about them. CUFC will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, CUFC will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection;
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice;
- Everyone processing personal information is appropriately trained to do so;
- Everyone processing personal information is appropriately supervised;
- Anybody wanting to make enquiries about handling personal information knows what to do;
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information;
- It will regularly review and audit the ways it hold, manage and use personal information;
- It regularly assesses and evaluates its methods and performance in relation to handling personal information;
- All staff are given a copy of this Data Protection Policy;
- 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.
- Any 3rd parties who have access to personal data will be checked for their IT security processes to ensure they comply with the EU General Data Protection Regulation 2018 and ensure a contract is in place specifying requirements around the confidentiality of information.

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 EU General Data Protection Regulation 2018.

Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information CUFC will hold and how it will be held or used.

EU General Data Protection Regulation 2018 – The EU Regulation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that CUFC follows its data protection policy and complies with the EU General Data Protection Regulation 2018..

Individual/Service User – The person whose personal information is being held or processed by CUFC, for example: a client, an employee, or supporter.

Explicit consent – Freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

Notification – Notifying the Information Commissioner about the data processing activities of CUFC, as certain activities may be exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the EU General Data Protection Regulation 2018.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within (GROUP).

Sensitive data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings