Castlemilk Community Football Trust
Registered Charity SC052014

Data Protection Policy

Introduction

This policy aims to ensure that [organisation] meets the legal requirements of the Data Protection Act 2018 – this is the UK's implementation of the General Data Protection Regulations (GDPR) standard.

Castlemilk Community Football Trust needs to collect and use certain types of information about the Individuals and service users who come into contact with us in order to carry on our work. Some of this information is personal information and must be collected and dealt with appropriately whether is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the Data Protection Act 1998.

Data Controller and Processor

In many cases Castlemilk Community Football Trust is the Data Controller under the Act, which means that it determines what purposes personal information held 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.

For some of our work we are the Data Processor, which means we process personal information on behalf of an external Data Controller, and for some of our work we are joint Data Controllers with an external body.

Where we are a data controller, and we contract with third parties to undertake some element of data processing we will ensure that each third party signs a Data Agreement with us to ensure they comply with the requirements of this policy in keeping data safe and secure and for using the data only for the purposes for which it was intended.

Disclosure

Castlemilk Community Football Trust may share data with other agencies such as funding bodies and partners.

Users will be made aware how and with whom their information will be shared. There are circumstances where the law allows us 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
- Providing a confidential service where the Individual'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 to provide consent signatures.

We regard 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.

It is our policy to ensure that personal information is treated lawfully and correctly. To this end, we will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 1998. We will ensure 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 Act, 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 Act,
- 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 in relation to the processing of personal information.

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

- Observe fully the conditions regarding the fair collection and use of information
- Meet our 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 fulfil our 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 Act. 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
- 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

Data Collection

Informed consent is when:

- An individual 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.

We 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, or online.

When collecting data, we will ensure that the individual:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the individual 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

Data Storage

Information and records will be stored securely and will only be accessible to authorised staff and volunteers. Information will be stored for only as long as it is needed or required by statute or our funders and will be disposed of appropriately.

It is our 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.

Data Access And Accuracy

All individuals have the right to access the information we hold about them. We will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes at the appropriate interval.

In addition, we will ensure that:

- We have a named 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
- We deal promptly and courteously with any enquiries about handling personal information
- We describe clearly how we handle personal information
- We will regularly review and audit the ways we hold, manage and use personal information
- We regularly assess and evaluate our methods and performance in relation to handling personal information
- 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 Data Protection Act 1998

Data Breach

If you become aware of any data breach or possible data breach then you should contact the Data Protection Officer immediately (in their absence, [the senior staff member/chair]). They will then talk to you about the nature of the breach (or suspected breach), assess the risks and take the appropriate action. The following actions may be taken:

- Immediate risk assessment and mitigating action against any immediate further breaches (e.g. setting new passwords, etc)
- Detailed investigation on the nature and extent of the breach and possible causes
- Contacting individuals and/or organisations to inform them of the breach if necessary
- Assessing reportable breaches and inform ICO within 72 hours as necessary
- Taking action to stop any further breaches; this may include further training for staff

It is important that you inform us of any breach or suspected breach so that we can take the right action and meet our statutory duties.

Training

New employees must read and understand the policies on data protection as part of their induction.
All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the Organisation are trained appropriately in their roles under data protection legislation.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and Castlemilk Community Football Trust of any potential lapses and breaches of Castlemilk Community Football Trust policies and procedures.

In case of any queries or questions in relation to this policy please contact the Data Protection Officer:

John Harkins
Tel: 0141 634 5474
admin@ccftrust.co.uk

Policy Date : April 2024