Data Protection Policy

DATA PROTECTION POLICY

Introduction

This policy is written in accordance with the Data Protection Act, General Data Protection Regulation (GDPR) and any other relevant legislation. Charlton Athletic Community Trust (CACT) is registered under the Act as a Data Controller under number Z2867856.

Statement

In accordance with the Data Protection Act 2018 and General Data Protection Regulations (GDPR) (EU) 2016, CACT will meet it legal obligations concerning confidentiality and the data security standards by having the appropriate physical and technical measures in place to ensure the security of any data collected, contained or handled by its systems, employees and any third parties. Access to CACT's systems and information by all staff, contractors, sub-contractors, suppliers, is diligently monitored with the appropriate pre- security checks including contractual agreements that sets out the minimum security requirements for confidentiality, integrity, availability and accountability of CACT's information and systems.

Protective measures in place for the secure transfer of personal data to and from a 3rd party includes, secure email, password protection, and anonymization if applicable. Our purpose for holding personal data and whom we share it with, including the security controls in place to protect the data are outlined in this policy and Privacy Notice.

The Data Protection Act and GDPR help to protect personal data and place restrictions on CACT's ability to disclose personal data within the UK and overseas. Any questions about this policy, or requests for further information, should be directed to the Head of Governance and Support Services Kathy.Smart@cact.org.uk.

Purpose

The purpose of this policy is to set out CACT's commitment and procedures for protecting personal data, and individual rights and obligations in relation to personal data. CACT 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.

This policy applies to the personal data that is collected and processed for employees, job applicants, participants who attend programmes and courses, contractors, partners and other individuals to carry out its business and organisational functions. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

Definitions

Personal data is any information that can be used to identify an individual, for example, information such as name, date of birth, email address, postal address, telephone number, etc. It also applies to personal data held in photographs or video clips (including CCTV). It includes data held on in any system or format, electronic or manual.

Special categories of personal data is any information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Criminal records data is any information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Processing includes obtaining, recording, organising, using, disclosing, deleting, and simply holding data so therefore in practice, anything done with data will amount to processing.

CACT may collect personal information when you register on CACT programmes or activities, pay for courses, request information, make a donation, subscribe to Newsletter or otherwise provide CACT with personal information.

CACT is committed to processing personal data in accordance with the following Data Protection Principles:

- Personal data is processed fairly, lawfully and in a transparent manner
- Personal data is obtained only for specified, explicit and legitimate purposes
- Personal data that is collected for the purpose of processing is adequate, relevant and limited to what is necessary
- Personal data is accurate and all reasonable steps will be taken to ensure that inaccurate personal data is rectified or deleted without delay
- Personal data is not to be kept for longer than is necessary for the purpose of processing
- Personal data is kept secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage

Data subjects will be clearly informed of the reasons for processing their personal data, how such data will be used and the legal basis for processing. Personal data of individuals will not be processed for other reasons

CACT will:

- Inform individuals why personal information is needed and how it will be used
- Only share personal information with consent from the individual, or when it is necessary and legally appropriate to do so (please refer to Confidentiality section)
- Ensure when information including electronic or paper format is authorised for disposal, it is done appropriately and securely
- Ensure appropriate security measures are in place to safeguard personal information by adopting best practice e.g. strong password protection, secure networks, secure buildings where information in all formats is stored (please refer to CACT IT Security Policy)
- Respond to requests for access to personal information in line with the Data Protection Act and the GDPR
- Train staff so that they are aware of their responsibilities and of CACT's relevant policies and procedures.

Special Categories of Personal Data

Special category data is subject to stricter conditions for processing under the GDPR. As such, measures will be taken to ensure that special category data is handled appropriately.

Special category data can only be processed if it meets one of several conditions in addition to the conditions outlined above:

- explicit consent of the individual (that will be kept on file)
- contractual obligations of an individual or compliance with employment law
- processing in the vital interests of the individual (where the individual cannot give consent or it cannot reasonably be obtained) or another person, where the individual has unreasonably withheld consent;
- the data is necessary for medical purposes and processing is done by a health professional or someone subject to an equivalent duty of confidentiality
- processing for the monitoring of equality of opportunity;

Confidentiality

CACT treats all personal information as confidential however; confidentiality may be broken in exceptional circumstances:

- When there is a serious risk of harm or abuse to an individual or someone else
- To protect others, for example, information about possible child abuse should be disclosed to the appropriate agency, (see CACT's Safeguarding Policy).
- To prevent a serious criminal act, especially where others may be endangered, for example an act of terrorism.

There is no obligation in general to pass on knowledge of a crime; however it is a criminal offence to:

- Deliberately mislead the police
- Receive a reward of any kind in return for not notifying the police about a criminal act
- Fail to notify the Police about an act that could be construed as an act of terrorism
- Fail to notify the Police about an act that could be construed as drug trafficking
- Knowingly take monies from a benefits agency fraudulently.

If a member of staff has to break confidentiality, the person must be informed and only do so after all attempts to persuade the individual have failed. A member of the Executive Team must be consulted will be responsible for making the final decision about the disclosure.

Consent

CACT will never sell personal information to third parties or share information without consent that will be held on file. You will be given an option to "opt-in" if you wish to receive further communication or information from CACT or Charlton Athletic Football Club. You will be able to select preferred method of communication:- Email, Telephone, SMS or mail. Electronic communications will always give you the option to unsubscribe or you can request this by telephone or in writing.

Individual rights
Individuals have a number of rights in relation to their personal data.

Subject access requests
Individuals have the right to make a subject access request. If an individual makes a subject access request, CACT will inform them:

- Whether or not their data is processed and if so why, the categories of personal data concerned and the course of the data if it is not collected from the individual;
- To whom their data is or may be disclosed, including recipients located outside of the European Economic Area (EEA) and the safeguards that apply to such transfers;
- For how long their personal data is stored (or how that period is decided);
- Their rights to rectification or erasure of data, or to restrict or object to processing;
- Their right to complain to the Information Commissioner if they think CACT has failed to comply with their data protection rights; and
- Whether or not CACT carries out automated decision-making and the logic involved in any such decision-making.

CACT will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

Subject access requests should be made in writing to the Head of Governance and Support Services. CACT may need to ask for proof of identification before the request can be processed. CACT will inform the individual if it needs to verify their identity and the documents it requires.

CACT will normally respond to a request within a period of one month from the date it is received. In some cases, such as where CACT processes large amounts of the individual's data, it may respond within three months of the date the request is received. CACT will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, CACT is not obliged to comply with it. Alternatively, CACT can agree to respond but will charge a fee which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which CACT has already responded. If an individual submits a request that is unfounded or excessive, CACT will notify the individual that this is the case and whether or not the request will be responded to.

Other rights
Individuals have a number of other rights in relation to their personal data. They can require CACT to:

- Rectify inaccurate data;
- Stop processing or erase data that is no longer necessary for the purposes of processing;

- Stop processing or erase data if the individual's interests override CACT's legitimate grounds for processing data (where CACT relies on its legitimate interests as a reason for processing data);
- Stop processing or erase data if processing is unlawful;
- Stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override CACT's legitimate grounds for processing data.

To ask CACT to take any of these steps the individual should send the request to the Head of Governance and Support Services.

Data security

CACT takes the security of all personal data seriously. CACT has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where CACT engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Responsibilities

CACT's Board of Trustees will approve the Data Protection Policy and is responsible for ensuring that sufficient resources are provided to support the requirements of this policy and related policies

The Information Governance Steering Group, comprise the CEO, Executive Team, Head of Governance and Support Services, Head of Health Improvement, Head of Fundraising and Development and Head Research and Development is responsible for overseeing all aspects of Information Governance; developing and maintaining related policies, standards, procedures and guidance, training and raising awareness of best practice. Meetings of the Information Steering Group take place quarterly, with additional meetings if required.

Managers within CACT are responsible for ensuring that the Data Protection Policy, related policies and guidelines are built into local processes and that there is on-going compliance

Processing of some personal data may carry a high risk to an individual's rights and freedoms, and in such cases CACT will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

Any actual, or suspected breach in personal data security, "near miss" or working practices which may jeopardise the security of personal data held by CACT must be reported in line with CACT's reporting of breach procedures, outlined in CACT's IT Security Policy and

breaches are recorded centrally, investigated and lessons learnt shared with staff. All breaches will be recorded regardless of their effect.

If CACT discovers that there has been a breach that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery.

If the breach is likely to result in a high risk to the rights and freedoms of individuals it will tell all affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures that have been taken.

Reporting Loss or Theft of Personal Information (Data Breach)

All incidences of loss or theft of personal or confidential information must be reported to your line manager and the Head of Governance and Support Services as soon as possible, as the breach may need to be reported to the ICO within 72 hours. A written report/ email should be submitted containing:

- Details of incident
- Date of discovery of incident
- Place of incident
- Who discovered the incident
- Action taken to mitigate risk to organisation
- Any further action taken by the person discovering the incident at the time of discovery

All breaches are recorded and actioned as appropriate. An investigation will be instigated and a decision taken whether the breach needs to be reported to a regulatory body or other third party, e.g. insurers, Information Commissioners Office, Charity Commission etc.

A central register of all incidents including "near miss" breaches is maintained by the Head of Governance and Support Services and reviewed by the Information Governance Steering Group quarterly. Lessons learnt are actioned and staff updated.

Individual responsibilities

Individuals are responsible for helping CACT keep their personal data up to date. Individuals should inform the HR Co-ordinator if data they have provided changes, for example if an individual moves house or changes bank details.

Individuals may have access to the personal data of other individuals and of our service users and partners in the course of their employment, contract, volunteer period, internship or apprenticeship.

Where this is the case, CACT relies on individuals to help meet its data protection obligations to staff, service users and partners.

Individuals who have access to personal data are required:

- To access only data that they have authority to access and only for authorised purposes;
- Not disclose data except to individuals (whether inside or outside CACT) who have appropriate authorisation;
- To keep all data secure, including electronic and paper records containing information (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- Not to remove personal data, or devices containing or that can be used to access personal data, from CACT 's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- Not to store personal data on local drives if working at other CACT locations
- Do not use personal devices without permission from your line manager

Further details about CACT's security procedures can be found in its data security policy.

CACT staff who fail to observe these requirements may be subject to a disciplinary investigation, which will be dealt with under CACT's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or service user data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

CACT staff will as a minimum training requirement complete certificated Data Protection and Information Sharing and Processing modules and annual refresher training. Those individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them. All CACT staff are responsible for making informed decisions to protect and properly manage personal data. CACT staff are responsible for ensuring that they are aware and understand the requirements of the Policy and for ensuring compliance on a day-to-day basis. Failure to comply with this and related policies may result in Disciplinary action.

CACT acknowledge that information is a valuable asset and will ensure that the information it holds, in whatever form, is appropriately managed and stored to protect the interests of individuals and stakeholders.

Policy review

The policy will be reviewed and approved by the Board of Trustees on an annual basis or sooner if required e.g. where there are changes in legislation, or recommended changes to improve best practice.

Drafted: March 2016	**Approved:** March 2016
Review: March 2017	**Approved: March 2017**
Review: March **2018**	**Approved: June 2018** (updated to reflect GDPR requirements)

Reviewed: June 2019 Approved: July 2019
Next Review June 2020

Related Policies and Guidance

CACT Information Governance Policy
CACT Information Sharing Policy
CACT IT Security Policy
CACT Records Retention Policy
Clear Desk Guidance and Password Guidance