DATA PROTECTION POLICY

Introduction

This policy is written in accordance with the Data Protection Act 2018 (DPA) and General Data Protection Regulation (EU) 2016 (GDPR). Charlton Athletic Community Trust (CACT) (referred to in this policy as "we") is registered under the DPA as a Data Controller under number Z2867856.

Statement

In accordance with the GDPR and DPA, 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 third party includes, secure email, password protection, and anonymisation 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.

The GDPR and DPA 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 handling the Personal Data of our customers, suppliers, employees, workers and other third parties. CACT regards the lawful and correct treatment of Personal Data as very important to successful working, and to maintaining the confidence of those with whom we deal.

This policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, job applicants, participants who attend programmes and courses, contractors, partners and other Data Subjects.

This Privacy Standard applies to all of CACT's personnel ("you"). You must read, understand and comply with this policy when Processing Personal Data on our behalf and attend training on its requirements. This policy sets out what we expect from you for CACT to comply with applicable law.

Definitions

Data Controller *is the person or organisation that determines when, why and how to Process Personal Data. We are the Controller of all Personal Data used by CACT.*

Data Subject *is a living, identified or identifiable individual about whom we hold Personal Data.*

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 or Special Category Data *is any information revealing an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation and biometric data.*

Criminal Convictions Data *is any information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.*

Processing, Processed or Process *any activity that involves the use of Personal Data. It includes obtaining, recording, organising, using, disclosing, deleting, and simply holding data so therefore in practice, anything done with data will amount to Processing.*

Related Policies *are CACT's policies, operating procedures or processes related to this policy and designed to protect Personal Data.*

Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject. CACT may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. CACT may collect Personal Data when you register on CACT programmes or activities, pay for courses, request information, make a donation, subscribe to our newsletter or otherwise provide CACT with your Personal Data.

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 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 where necessary kept up to date
- Personal Data is not to be kept for longer than is necessary for the purpose of Processing

- Personal Data is Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage
- not transferred to another country without appropriate safeguards being in place
- made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data

CACT is responsible for and must be able to demonstrate compliance with the data protection principles listed above

CACT will:

- Inform individuals why personal information is needed and how it will be used, providing detailed, specific information
- Not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless the Data Subject has been informed of the new purposes and they have consented where necessary
- 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 in this policy on page 4)
- Ensure Personal Data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed
- Ensure when information including electronic or paper format is authorised for disposal, it is done appropriately and securely
- Not keep Personal Data in an identifiable form for longer than is necessary for the purposes for which the data is Processed, taking all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with CACT's retention schedules and policies
- 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'S IT Security Policy)
- Ensure that Personal Data is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards, taking all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data
- Respond to requests for access to personal information in line with the GDPR and DPA
- 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
- Were required by law or regulatory body

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, a member of the Executive Team must be consulted and will be responsible for making the final decision about the disclosure.

Consent

CACT will only Process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include consent.

When Processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for Processing if possible. Where consent is relied on, you must issue a notice to the Data Subject to capture it.

You will need to evidence consent captured and keep records of all Consents in accordance with Related Policies.

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.

DATA SUBJECT'S 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

CACT will also provide the individual with a copy of their Personal Data held by CACT. 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 Data Subject's Personal 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:

- Withdraw consent to Processing at any time
- Receive certain information about the Data Controller's Processing activities
- Rectify inaccurate data or to complete incomplete data
- Stop Processing or erase data that is no longer necessary for the purpose for which it was collected or Processed

- Challenge Processing which has been justified on the basis of our legitimate interests or in the public interest
- Stop Processing or erase data if Processing is unlawful
- Restrict Processing in specific circumstances
- Request a copy of an agreement under which Personal Data is transferred outside of the EEA
- Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else
- Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms
- Make a complaint to the supervisory authority
- In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format

To ask CACT to take any of these steps the Data Subject 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.

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 if appropriate the purposes for which the activity is carried out, the Data Controller's legitimate interests, an assessment of the risks to individuals, an assessment of the necessity and proportionality of the Processing in relation to its purpose 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 you know or suspect that a Personal Data breach has occurred, do not attempt to investigate the matter. Immediately contact the person or team designated as the key point of contact for Personal Data breaches (the Head of Governance and Support Services). You should preserve all evidence relating to the potential Personal Data breach.

Reporting Loss or Theft of Personal Information (Data Breach)

All incidences of loss or theft of personal or confidential information must be reported to line managers 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 and, in some instances, inform the Data Subject. 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.

Individuals responsibilities

Individuals are responsible for helping CACT keep their Personal Data up to date. Individuals should inform the HR Co-ordinator if Personal Data they have provided changes.

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
- 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 CACT's IT 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 Policy. 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.

Responsibilities

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

The Information Governance Steering Group, comprises the Executive Team and members of the Senior Management Team, is responsible for overseeing all aspects of Information Governance, developing and maintaining all related policies, standards, procedures and guidance, training and raising awareness of best practice. Meetings of the Information Steering Group are scheduled annually and take place quarterly, with additional meetings if required. The Board of Trustees receive and discuss minutes of the meetings at their quarterly Board meetings.

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

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.

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 all 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
Reviewed: September 2020
Next Review: September 2021

Related Policies and Guidance

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