Data Protection & Security Policy 2018-19

Crawley Town Community Foundation

Data Protection & Security Policy Statement

Crawley Town Community Foundation (CTCF) will do everything within our power to ensure the protection and security of any data of a personal or sensitive nature.

CTCF is intent on providing the safest online experience, and are therefore committed to protecting your privacy with an appropriate form of data capture. We will ensure that any data held is as up to date and accurate as possible, and any inaccuracies corrected without unnecessary delay.

Data held will not be disclosed to a third party without the appropriate consent by parents/carers and those of an age to provide consent or unless we are required to do so. Please refer to our Privacy Statement within our GDPR (General Data Protection Regulation) Statement's document.

Data provided is held in a secure format either electronically or paper and only authorised staff have access to the data.

Data Access Subject requests may be made in writing to see part or all the personal data held by CTCF. Please refer to the Confidentiality and Information Sharing Policy when reading this Policy.

Introduction

It is important there is a clear personal data handling policy to avoid or at least minimise the risk of personal data breaches. A breach may arise from a theft, a deliberate attack on our system, the unauthorised use of personal data by a member of staff, accidental loss, or equipment failure.

In addition:

- No individual would want to be the cause of any data breach, particularly as the impact of data loss on individuals can be severe and cause extreme embarrassment, put individuals at risk and affect personal, professional or organisational reputation

- We will want to avoid the criticism and negative publicity that could be generated by any personal data breach

- We are subject to a wide range of legislation related to data protection and data use, with significant penalties for failure to observe the relevant legislation including criminal prosecution and fines imposed by the Information Commissioners Office (ICO).

Increasingly data is held digitally but also in paper form.

Legislation covering the safe handling of this data was mainly through the Data Protection Act (DPA) (1998). However, this will be superseded through new UK legislation following the European GDPR (2016). Given the personal and sensitive nature of much of the data held, and with moving increasingly more into a digital era, it is critical that the new legislation is adopted.

This includes all forms of personal data and personal sensitive data, regardless of whether it is held on paper or in electronic format.

We do everything within our power to ensure the safety and security of any material of a personal or sensitive nature. All forms of data-collection, including consent and monitoring and evaluation, will be systematic and supported through this framework.

It is the responsibility of all members of staff to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in data protection legislation, regulations and guidance.

We have presented a set of rules for the processing and security of personal data (both manual and digital records). It provides individuals (data subjects) with rights of access, privacy and correction. It defines the responsibility of data controllers, for those responsible (either alone or jointly or in common with other persons) for the manner any personal data is processed. It also describes the role of the data processor in relation to personal data, that is any person (other than an employee of the data controller) who processes the data on behalf of the data controller (For example our IT provider, Substance Views and Official Soccer School website).

Personal and Sensitive Personal Data

Personal data is any information relating to an identified or identifiable natural person (data subject), directly or indirectly, particularly in reference to an identifier such as a name, ID number, location data, an online identifier, or to one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Sensitive Personal Data

These relate to special categories of personal data, including information about racial or ethnic origin, political opinions, racial beliefs, sexual orientation, health and genetic data.

Data Capture

CTCF uses both online and paper data capture and is committed to ensuring that data held secure and accurate.

We will have access to a wide range of personal information and data. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include personal information about participants – e.g. names, addresses, contact details, legal guardianship contact details, attendance records etc. Records are kept and maintained to provide the data subject the most professional, safe and secure programme and service possible.

Responsibilities

Please refer to our Security Statement within our GDPR Statement's document when reading this section. Data Controller refers to the application of responsibility for the security of data. By definition, CTCF is the data controller as it collects and stores personal information. The Foundation CEO has overall responsibility to inform and advise all staff of policy and procedure when handling personal and sensitive data. Every member of staff has the responsibility of handling personal and sensitive data in a safe and secure manner. Regular meetings and training will be held to review policy and procedure, and so that all staff are aware of the importance of data security.

The Board of Trustees are required to comply with this policy with having overall responsibility of CTCF, and in the event that they have access to personal data when engaged in their role as Trustee.

It is the responsibility of all staff to preserve the confidentiality of data held. This can be achieved by setting the IT screen saver auto lock, using strong passwords that are changed regularly through the Foundation's IT provider, not disclosing passwords to other members of staff, avoiding access to data the staff member does not have authorisation to, and maintaining a clear desk policy to avoid loss or disclosure.

All staff are responsible to follow these guidelines to avoid any breaches of data security. Any staff unsure of any part of data protection and security should seek clarification and act accordingly on the information given to them. Staff will be notified of any changes in legislation and the impact on data protection and security, and will be required to implement the necessary changes.

The Data Processor must only act on the written instructions of the controller (unless required by law to act without such instructions). The Processor must ensure that people processing the data are subject to a duty of confidence. The Processor must take appropriate measures to ensure the security of processing. The Processor must only engage a sub-processor with the prior consent of the data controller and a written contract. The Processor must assist the Data Controller in providing subject access and allowing data subjects to exercise their rights under the GDPR. The Processor must assist the Data Controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments. The processor must delete or return all personal data to the controller as requested at the end of the contract.

Staff and Remuneration for Admin and Data-Entry Roles

Staff are responsible for administration of data and entering data as much as their time allows it. In the instance that the collection of data becomes too great for this to be possible, the Foundation will assess employing a member (s) of staff for data-entry. Indeed, this has been implemented through the employment of staff members whose main focus is with regards data entry, with overall responsibility on their line managers.

Registration

The Foundation is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information Sharing and Rights of Access

Please refer to our Rights of Access Statement in the GDPR Statement's document when reading this section. In order to comply with processing requirements, we request consent from parents / carers / guardians of data we collect, process and store of minors. We inform adults of the purposes for which data is held, how it will be used, and to whom it may be passed to (also see our Confidentiality and Information Sharing Policy).

Information Sharing and Consent

We aim to ensure that personal information is shared securely and appropriately. The circumstances in which information can be shared is explained to participants and / or parents at registration and when they sign a form to confirm they understand the circumstances of when information may be shared without their consent.

We are obliged to share confidential information without authorisation from the person who provided it or to whom it relates, if it is in the public interest.

This could be to prevent a crime from being committed or to intervene where one may have happened, for health related reasons, or to prevent harm to a child or adult; or when not sharing it could be worse than the outcome of having shared it.

The decision should never be made as an individual, but with the support of relevant agencies.

The three critical criteria are:

- Where there is evidence that the child / adult at risk is suffering, or is at risk of suffering, significant harm.
- Where there is reasonable cause to believe that a child / adult at risk may be suffering, or at risk of suffering, significant harm.
- To prevent significant harm arising to children and young people or serious harm to adults, including health related circumstances and the prevention, detection and prosecution of serious crime.

(Refer to our Safeguarding policies for Children and Young People, and Adults at Risk).

Consent

Consent will be either via a website consent form or in a paper format.

All requests for consent must be concise and clear to understand.

Both options will require the positive action to opt in or opt out.

When requesting consent the data subject must be made aware of how the data will be processed.

The data subject will only be asked for information for the specific programme they will participate in. The Foundation does not use information given for one programme to be used on another, as explicit consent is required for all programmes. The data subject must consent

The data subject must also be made aware of how the information will be held, either electronically, paper or both. The data subject will be informed if any of the information given will be shared to third parties and why.

The website booking form also contains our policy and privacy statement.

Training & Awareness

All staff will receive relevant data protection and security policy training, and will be made aware of their responsibilities, including other training, use of IT systems, and working with data processing agencies.

Data Access and Portability

The Data Controller works with Crawley Town FC and the IT Provider, as well as guides staff, to update and manage systems, including the use of usernames, passwords and encryption to prevent unauthorised access to personal and sensitive information. This includes the setting of access levels, passwords (and changes to passwords) and security settings, and updating systems and programmes to avoid any corruption to files. This includes any security/malware software and the continuous monitoring of the software.

The Data Controller, Crawley Town FC and the IT provider are to liaise to ensure that the Foundations system is secure; and the IT provider is always available by phone. The main server is backed up hourly between 9am and 6pm to a Network Attached Storage device and then moved at 11pm to the offsite data storage of the IT provider.

We will ensure that IT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are ordered and accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will have strong passwords, which should be changed regularly. User passwords must never be shared.

Wherever possible the use of encryption should be used when sending Personal (and personal sensitive) data to or from a third party via email (Egress). Registration is required. Staff should contact the Data Controller if they are unsure of what services are available or to get a service activated.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage for media and portable electronic equipment must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation, and managed in accordance with data protection legislation.

Private equipment (i.e. owned by the users) must not be used for the storage of personal data held by CTCF. Personal email accounts must not be used for CTCF operational purposes and with regards personal (and sensitive) data. This applies to all trustees.

Subject Access Requests

Written request to see all or part of the personal data held by the Data Controller in connection with the data subject can be made. Data subjects have the right to know if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them.

Under certain circumstances, the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

CTCF will keep information on the data subject for a maximum period of 10 years. The length of time was determined by the fact that there are medical records and safeguarding information and data that may be required and requested from suitable third parties over the length of time. These include the emergency and other professional services.

Physical Security

Visitors to our premises are supervised by a member of staff and the offices are alarmed overnight, which prevents or at least minimises the risk of personal data breaches. All staff are aware of using and protecting log in and password information, and lap tops and memory hardware is locked or taken away overnight.

Staff are advised of how to use data securely when using a mobile device, and on measures to minimise the risk of them being stolen. All paper copies containing data are locked away into filing cabinets, and any unwanted paperwork is destroyed using a shredder.

Third Party Security

We seek permission and consent from the data subject we have personal information from and when their data might be used by a third party, including Crawley Town FC. We have the overall responsibility of the data handled by third parties, and so therefore we have the following preventative measures in place to prevent any breaches:

-Review the third party policy regarding data handling and use;

-Incorporate measure within contractual agreements that stipulates where and how data should be processed;

-Understand and monitor third party use of our data

Disposal of Data

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with legislation, and other media must be shredded, incinerated or otherwise disintegrated for data.

Breaches

All staff and contractors have a responsibility for reporting information, security incidents or breaches of information, confidentiality to the Data Controller and the Deputy Data Controller and a suitable trustee. When reporting an incident, the Data Controller and the Deputy Data Controller and a suitable trustee will record the breach in the data security breach log. All staff and contractors must ensure that sufficient information is given to allow the incident to be investigated and wherever possible the risk of recurrence minimised or eliminated. Any serious personal data breaches must be reported as soon as is practically possible (within 72 hours), providing full details of the nature and extent of the breach.

The UK's independent authority set up to uphold information rights in the public interest promoting openness by public bodies and data privacy for individuals is the Information Commissioner's Office.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

https://ico.org.uk/

The Data Protection and Security Policy of Crawley Town Community Foundation is endorsed by the Board of Trustees (who have overall responsibility) and reviewed on an annual basis or when legislation changes.

Any amendments to the policy are covered in the Sub Group Meetings, Board Meetings, and advised to staff in Team Meetings.