CRiBS Data Protection Policy

Introduction

CRiBS is committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of Data in order to carry on our work. This personal information must be collected and dealt with appropriately. The Data Protection Act 1998 (DPA) and the General Data Protection Regulations govern the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs. The charity will remain the data controller for the information held. The trustees, staff and volunteers will take responsibility for processing and using personal information in accordance with all relevant legislation. Trustees, staff and volunteers who have access to personal information, will be expected to read and comply with this policy.

Purpose

The purpose of this policy is to set out CRiBS Charitable Trust's commitment and procedures for protecting personal data. The trustees 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.

The General Data Protection Regulations

This contains 7 principles for processing personal data with which we must comply.

Personal data:

1. Must be processed lawfully, fairly and transparently
2. Can only be collected for specified, explicit and legitimate purposes
3. Must be adequate, relevant and limited to what is necessary for processing
4. Shall be accurate and kept up to date
5. Shall not be kept for longer than is necessary,
6. Shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Approved 5th October 2020

7. The data controller will be accountable for complying with the principles, and to have appropriate processes and records in place to demonstrate that CRiBS is compliant.

Definitions

Data Controller – The person who (either alone or with others) decides what personal information CRiBS will hold and how it will be held or used.
Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.
Data Protection Officer – The person on the management committee who is responsible for ensuring that it follows its data protection policy and complies with the Data Protection Act 1998.
Data Subject/Service User – The individual whose personal information is being held or processed by CRiBS, for example: a service user or a supporter
'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about her/him.
Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.
Processing – means collecting, amending, handling, storing or disclosing personal information.
Personal Information – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses.

Collecting and correcting data

Whenever CRiBS staff or volunteers collect personal data from members of the public, we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose.

Individuals have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them.

Responsibilities

CRiBS is the Data Controller, and is legally responsible for complying with the GDPR and all relevant legislation, which means that it determines what purposes personal information held will be used for. CRiBS will take into account legal requirements, and will through appropriate management, strict application of criteria and controls:

a) Observe fully conditions regarding the fair collection and use of information.
b) Meet its legal obligations to specify the purposes for which information is used.
c) Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements.
d) Ensure the quality of information used.
e) Ensure that the rights of people about whom information is held, can be fully exercised. These include: i) The right to be informed that processing is being undertaken ii) The right of access to one's personal information iii) The right to prevent processing in certain circumstances, and iv) The right to correct, rectify, block or erase information which is regarded as wrong information

f) Take appropriate technical and organisational security measures to safeguard personal information,
g) Ensure that personal information is not transferred abroad without suitable safeguards,
h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
i) Set out clear procedures for responding to requests for information.

The Data Protection Officer on the management committee is: Mark Leveson

Contact Details: mark@cribsonline.org

The Data Protection Officer will be responsible for ensuring that the policy is implemented and will have overall responsibility for:
a) Everyone processing personal information understands that they are contractually responsible for following good data protection practice
b) Everyone processing personal information is appropriately trained to do so
c) Everyone processing personal information is appropriately supervised
d) Anybody wanting to make enquiries about handling personal information knows what to do
e) Dealing promptly and courteously with any enquiries about handling personal information
f) Describing clearly how the charity handles personal information
g) Regularly reviewing and auditing the ways CRiBS holds, manages and uses personal information
h) Regularly assessing and evaluating CRiBS methods and performance in relation to handling personal information.

All staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to 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. In case of any queries or questions in relation to this policy please contact the Data Protection Officer.

Data collection: Informed consent

Informed consent is when a Data Subject 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.

When collecting data, we will ensure that the Data Subject:

a) Clearly understands why the information is needed
b) Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
e) Has received sufficient information on why their data is needed and how it will be used

Procedures for Handling Data & Data Security

CRiBS has a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- unauthorised or unlawful processing of personal data
- unauthorised disclosure of personal data
- accidental loss of personal data

All staff must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper or in a computer or recorded by some other means.

Personal data relates to data of living individuals who can be identified from that data and where use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs etc. would be classed as personal data.

It is therefore important the all staff consider any information that can be used to identify an individual as personal data and observe the guidance given below.

Operational Guidance for CRiBS staff/volunteers (to be incorporated in staff handbook)

Email:

All staff should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or, printed and stored securely. The original email should then be deleted from the personal mailbox and any "deleted items" box, either immediately or when it has ceased to be of use.

Remember, emails that contain personal information which is no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

Phone Calls:
Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- If you receive a phone call asking for personal information to be checked or confirmed, be aware that the phone call may come from someone pretending to be the data subject, or impersonating someone with a right of access.
- Personal information should not be given out over the telephone unless you have no doubts as the caller's identity and the information requested is innocuous. If you have any doubts, ask the caller to put their enquiry in writing.

Laptops and Portable Devices:

All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program.
Ensure your laptop is locked (password protect) when left unattended, even for short periods of time.

When travelling in a car, make sure the laptop is out of sight, preferably in the boot. If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.
Never leave laptops or portable devices in your vehicle overnight. Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you

Data security and storage:

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on CRiBS cloud based storage system. The disk or memory stick should then be securely returned (if applicable) or processed for safe storage or disposal. The underlying principle is that, wherever possible, personal data should be held only in CRiBS cloud based storage and not on personal laptops or office computer hard drives.

Always lock (password protect) your computer or laptop when left unattended; this is especially important when using your laptop away from the office.

Passwords:

Do not use passwords that are easy to guess. Make sure all of your passwords contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.

Protect Your Password:

Common sense rules for passwords are:
do not give out your password
- do not write your password somewhere on your laptop
- do not keep it written on something stored in the laptop case

Data Storage

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

Approved 5th October 2020

Information will be stored for only as long as it is needed or required statute 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.

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 Subject Access Requests

Individuals have a right to access their personal data as well as other supplementary information. They can make a request verbally or in writing including via email or social media. CRiBS' management understand that they have one month to respond to a request and will not charge a fee for providing a response. We are aware there are some situations where we may extend the time limit to respond to a request.

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone).

CRiBS management will refer to the Guide to GDPR checklist to ensure Data Subject Access Requests are processed correctly and effectively.

Risk Management

The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Volunteers should be aware that they can be personally liable if they use customers' personal data inappropriately.

This policy is designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.

This policy is reviewed annually.

Approved 5th October 2020