Churches Together in Bexhill (CTiB)
Data Protection Policy

Introduction:

Bexhill Foodbank collects and uses information about the Data Subjects with whom we come into contact in order to carry out our work. This information must be collected and dealt with appropriately – whether on paper, electronically, or recorded on other material - and there are safeguards to ensure this under the Data Protection Act 1998 and in compliance with the General Data Protection Regulations.

Data Controller:

CTiB is the Data Controller under the Act, and will determine what purposes the information held will be used for. CTiB is also responsible for notifying the Information Commissioner of the data we hold or are likely to hold, and the general purposes that this data will be used for.

Disclosure:

CTiB will not disclose personal information to a third party unless we believe it is lawful to do so. We will not pass on personal details to anyone outside the foodbank for marketing purposes. There are particular circumstances where the law allows {Named charity} to disclose data without the data subject's consent:

1. Carrying out a legal duty as authorised by an appropriate legal officer
2. The Data Subject has already made the information public
3. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
4. Where there is a "legitimate interest", such as preventing abuse of the system by those trying to obtain more foodbank vouchers than they are entitled to

CTiB places great importance on the correct treatment of personal information and recognise that this plays a key part in retaining the trust and confidence of those with whom we work and serve. We will strive to ensure that personal information is always treated lawfully and correctly.

CTiB is registered with the Information Commissioner's Office and will continue to do so on an annual basis.

Adherence to Data Protection Legislation:

To this end CTiB will, through appropriate management and strict application of criteria and controls, adhere to the principles of the Data Protection Act 1998 and General Data Protection Regulations, which require that:

1. personal data should be processed fairly and lawfully
2. data should be obtained only for one or more specified and lawful purposes
3. the data should be adequate, relevant and not excessive
4. data should be accurate and, where necessary, kept up-to-date
5. data should not be kept for longer than necessary
6. personal data should be processed in accordance with individual's rights under the Act
7. data should be kept secure
8. personal data should not be transferred outside the European Economic Areas unless the country offers adequate data protection

Data subjects:

CTiB holds personal data about a number of groups of data subjects, including (but not necessarily limited to):

- Employees of the charity
- Volunteers of the charity
- Trustees of the charity
- Financial donors to the charity
- Supporters of the charity
- Clients receiving emergency food assistance
- Clients providing case study information to the charity
- Local contacts (referral agencies, food donor groups, other client support services etc)
- Complainants

Data Privacy Statements:

CTiB maintains an up-to-date "data privacy statement" for each of its principal groups of data subjects. Data privacy statements are available separately, and are freely available to data subjects on request. They provide the following specific information for the relevant group of data subjects:

- What personal data **CTiB** holds
- How the personal data is kept safe
- What the data is used for
- The "lawful basis" (legal right) of CTiB to hold and process the data
- Who can see the data
- How long the data will be kept
- The data subjects' rights

Data subjects' rights:

CTiB is committed to upholding the rights of data subjects, particularly:

- Right to be know what data is held
- Right to have a copy of the data held
- Right to object to the "lawful basis" for holding data
- Right to object to the misuse of data
- Right to have data corrected
- Right to be forgotten (to have data removed)

Foodbank client data collection:

The bottom of each printed foodbank voucher contains a data statement. An equivalent statement is to be read to any clients being referred by the "e-referral" process. This statement makes clear:

- the charity's commitment to data security
- the "lawful basis" for holding and processing client data
- the client's data will be retained for statistical analysis
- to help prevent misuse, the dates and locations of foodbank visits may be shared
- client data will not be used for any other purposes
- it will only be seen by people that need to do so for foodbank reasons
- it is never sold or given to any other body

By presenting the voucher (or voucher code) at a foodbank, the client will be regarding as having accepted the associated data statement.

Other personal data collection:

When collecting any other data, **CTiB** will ensure that the Data Subject:

- understands why the information is needed, and the "lawful basis" for doing so
- understands what it will be used for and what the consequences are should the Data Subject decide not give consent to processing
- grants explicit written or verbal consent for data to be processed, where consent is required
- 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

CTiB 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.

Data Storage:

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

Personal data will be stored for only as long as it is needed or required by statute, or to satisfy Charity Commission auditing expectations, and will be disposed of appropriately and securely.

It is the charity's 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.

Subject access requests:

All Data Subjects have the right to make a "subject access request", to ask CTiB for details of the personal data held about them. If CTiB receives a "Subject Access Request", we will take the following actions within one month:

- Confirm if the charity holds any personal data about the data subject
- Provide them with a copy of that data
- Provide any supporting explanatory materials (e.g. a Data Privacy Statement)

If they wish to, the data subject can ask for a copy of their in a "commonly used electronic form" (e.g. a familiar file type, such as Excel, CSV, Word, PDF etc). This is their "Right to Portability".

The foodbank reserves the right to charge a reasonable fee where requests are "manifestly unfounded or excessive" and particularly if they are repetitive. No fee will normally be charged for a party's first SAR, or where previous SARs have found errors in their data. Where requests are "manifestly unfounded or excessive" and/or repetitive a typical fee will be £10. We reserve the right to increase this for further SARs to reflect the time taken in processing an SAR.

If a SAR reveals that any details we hold are incorrect, they will be amended and no fee will be charged.

CTiB 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.

Data breaches:

CTiB takes reported "data breaches" very seriously.

We will take prompt actions to investigate a suspected data breach, to minimise the effect of any breach, and to reduce the chance of it happening again. The actions will be recorded in a Data Breach Register. If a data subject contacts us about a breach involving their data, we will inform them of the actions taken.

The trustees of CTiB will be kept informed of any data breaches.

If we become aware of any data breach, we will always consider carefully whether it should be deemed a "serious breach".

If we believe there has been a serious breach, we will always

- report it promptly to the Information Commissioners Office
- take reasonable steps to contact or inform the data subjects whose data is involved
- report it to The Trussell Trust's governing body of charity trustees, with a copy of the incident record from our Data Breach Register.

Automated decision making and profiling:

CTiB **does** not use personal data for automated decision making and profiling.

In addition, CTiB will ensure that:

1. We have a nominated Data Protection Officer with specific responsibility for ensuring compliance with Data Protection requirements
2. Everyone processing personal information understands that they are contractually responsible for following good data protection practice
3. Everyone processing personal information is appropriately trained to do so
4. Everyone processing personal information is appropriately supervised or managed
5. Everyone with access to personal data in the foodbank data system will sign a Data Protection Statement, committing them to respect data security. A copy will be kept in each volunteers' and staff members' records.
6. We provide full, accurate and clear information about our handling of personal data in Data Privacy Statements for each significant group of data subjects
7. We make it easy for data subjects to ask for and receive a copy of the relevant Data Privacy Statement
8. We deal promptly and courteously with any enquiries about handling personal information
9. We will regularly review and audit the way we hold, manages and use personal information
10. We will regularly assess and evaluate our methods and performance in relation to handling personal information
11. All staff will be made 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 reviewed and 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.

The following list of definitions of the technical terms used is intended to aid understanding of this policy.

Data Breach - When personal data is used for a purpose that it wasn't intended for, or is shared with someone who wasn't intended to see it.

Data Controller – The person who (either alone or with others) decides what personal information is held, how it will be held, reported upon, processed 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 responsible for ensuring that the data protection policy complies with the Data Protection Act 1998 and is correctly applied

Data Subject/Service User – The individual whose personal information is being held or processed by CTiB (for example: a client, an employee).

'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. Explicit consent is needed for processing sensitive data.

Notification – Notifying the Information Commissioner about the data processing activities of CTiB as certain activities may be exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – Collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about companies and agencies but applies to named persons or employees within CTiB

Serious breach – A data breach that is "likely to result in a risk to the rights and freedoms" of the data subject(s). A "serious breach" is one which could be expected to have a negative impact on the people whose data has been misused.

Sensitive data – means data about:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal record
- Criminal proceedings relating to a data subject's offences