Data Security Policy

Last updated	March 2024
Review date	March 2025

Definitions

Charity	BCT Aspire
GDPR	means the General Data Protection Regulation.
Responsible Person	means the Chief Executive (currently Patrick Wilson)
Register of Systems	means a register of all systems or projects for which personal data is processed by BCT Aspire.

Policy statement

BCT Aspire requires all its employees and Board members who process or use any personal information from employment or customer records to comply fully with its Data Protection Policy and the principles of the Data Protection Act 2018 and UK GDPR. Disciplinary action may be taken against any employee or Board member who breaches any of the instructions or procedures following from the Policy.

BCT Aspire will collect and hold the minimum personal data necessary to enable it to perform its key tasks and the data willbe erased once the need to hold it has passed. Every effort will be made to ensure that data is accurate and the individual's rights will be upheld as outlined in guidance relating to the Data Protection Act 2018.

Responsibilities

BCT Aspire's Chief Executive is the Data Protection Officer, and they have responsibility for information and data protection in the organization. They are the designated Information Asset Owner (IAO).

Each system, or project, which BCT Aspire operates will have a System Owner, and a risk register, which includes consideration of the risks relating to personal data, and mitigation of each of these risks. The system owner will be responsible for maintaining the system's risk register.

Employees and Board members are responsible for:

• Ensuring any information they provide to BCT Aspire is accurate and up to date.

• To inform BCT Aspire of any changes to information they have previously provided e.g. changes of address, or errors.

• Complying with this data protection policy.

Line Managers are responsible for ensuring that all employees they supervise are aware of their responsibilities under the Data Protection Act 2018. Data Protection will be covered as part of all new staff induction.

If and when employees or Board members as part of their responsibilities collect, access and process information for projects, employment records or member information they must comply with the eight principles of the Data Protection Act 2018[1].

2. General provisions

a. This policy applies to all personal data processed by BCT Aspire.
b. The CEO shall take responsibility for BCT Aspire's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. BCT Aspire shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the following criteria applies:

   - The individual has given consent;
   - The processing is required for the individual to enter into a contract, or to have a contract set up, or is necessary to comply with any legal obligation other than that imposed by contract;
   - The processing is necessary in order to protect the vital interests of the data subject;
   - Processing is necessary for the administration of justice, exercise of functions conferred under an Act of Parliament, exercise of functions of the Crown, or the exercise of other functions of a public nature in the public interest.

[1] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

- Processing is necessary for the legitimate interests of the data controller, except where this may prejudice the rights and freedoms and legitimate interests of the data subject - this purpose may be regulated by specific orders of the Secretary of State.

In addition, certain types of data are considered to be "sensitive". Sensitive personal data is defined as one or more of the following pieces of data about the data subject:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs
- Membership of a Trade Union
- Health and/or medical information
- Sex life or sexual orientation;
- Genetic or biometric data

In order to process *sensitive* data, one or more of these criteria must also be met:

- the data subject has given explicit consent
- processing is necessary to comply with the law in connection with employment
- processing is necessary to protect the vital interests of the data subject or another person where consent cannot be given by the data subject
- processing is carried out for legitimate activities by any body which is not conducted for profit or exists for political, religious or trade union purposes, and carries out appropriate safeguards, relates only to members or regular contacts, and does not involve disclosure without the consent of the data subject
- the information has been made public as a result of steps deliberately taken by the data subject
- processing is necessary in connection with legal proceedings, obtaining legal advice or defending legal rights
- processing is necessary for the administration of justice, exercise of functions conferred by an enactment, exercise of any functions of the Crown
- processing is necessary for medical purposes and is undertaken by a health professional, or one with an equivalent duty of confidentiality
- processing information as to racial or ethnic origin is necessary for equal opportunity purposes, subject to appropriate safeguards for the rights and freedoms of the data subject
- any other purpose specified in an order made by the Secretary of State .

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Lawful, fair and transparent processing

To ensure its processing of data is lawful, fair and transparent, BCT Aspire shall maintain a Register of Systems. These are systems which can be used to process personal data.

a. The Register of Systems shall be reviewed at least annually. Each system will have an 'owner', and a risk register, which includes consideration of the risks relating to personal data, and mitigation of each of these risks. The system owner will be responsible for maintaining the system's risk register.
b. Individuals have the right to access their personal data and any such requests made to BCT Aspire shall be dealt with in a timely manner.

5. Lawful purposes

The lawful bases for processing are set out in Article 6 of the UK GDPR regulations. At least one of these must apply whenever BCT Aspire processes personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the

legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

- BCT Aspire shall note the appropriate lawful basis in the Register of Systems.
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent will be clearly available and systems will be in place to ensure such revocation is reflected accurately in BCT Aspire's systems.

6. Data minimisation

BCT Aspire shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

7. Accuracy

a. BCT Aspire shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

8. Data Retention

To ensure that personal data is kept for no longer than necessary, BCT Aspire shall put in place a retention policy for each system in which personal data is processed and review this policy annually. Each system will include a data retention statement, setting out what data should/must be retained, for how long, and why. There will also be reference to a process for deleting it.

9. Security

a. BCT Aspire shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security will be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this will be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

10. Data security

Personal data relating to external individuals is held digitally on the shared drive. Only BCT Aspire employees and our processors can access the data. Data on our shared drive can be accessed remotely as well as from computers in the office.

BCT Aspire ensures the security of our data through the following security measures:

• Staff PC passwords are changed on a regular basis

• Staff PC passwords for the remote working system are changed on a regular basis

• No one other than BCT Aspire employees and our processors can access our system.

• Personal data on our shared drive is separated into folders and permitted access is only granted to relevant staff members.

• Our processors only access our systems with the permission and knowledge of the person on the Service Level Agreement/contract.

• Our processors only access the data held on our systems when necessary to carry out the task required.

• Our processors are operating in a GDPR compliant environment and have confirmed this is the case.

All employees are responsible for ensuring that their passwords are secure and for not accessing or processing data in a manner which is contrary to this policy. BCT Aspire employees will not, for example, send data to their personal email addresses or to any third parties or take personal data off site.

When using portable devices, for example laptops, tablets and phones, to access data BCT Aspire employees and Board members will apply the same level of diligence when accessing from the office. Particular care should be taken when using portable storage devices, for example USBs, and if any personal data is stored on the portable device BCT Aspire employees and Board members will ensure it is encrypted. Password protection will be used for files as appropriate when remote working

HR files are stored in hard copy in secured files in the office. The keys for the filing cabinet are only accessible by the Chief Executive and the Finance Officer.

The BCT Aspire office is locked when there is no one in the office.

11. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, BCT Aspire shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

END OF POLICY

Appendix One: Data Protection responsibilities

BCT Aspire Board

- Be satisfied that a suitable Data Protection Policy is in place and that it is adhered to

CEO/Data Controller

- Review the Policy annually with the Board
- Hold Register of Systems and review annually
- Ensure BCT Aspire staff are aware of Data Protection responsibilities

System owners

- Define your system for holding and processing personal data
- Maintain system risk register and review annually with CEO

Appendix Two: Data Protection risk register for systems

(to be informed by BCT Aspire's Data Protection Policy)

Name of system / project:

Name of system owner:

Description of how the system works

What data about individuals is held?	Why is it needed?	Which lawful processes apply to this data?	When will the data be deleted?	Why will the data be deleted at that time?	Risk	Mitigation

Appendix Thee : document retention periods

We will retain documents for following periods of time:

Type of document	Retention period	Hard copy or electronic?
Health and Safety logs	5 years	Hard copy
Equipment maintenance certificates	5 years	Hard copy
Legionella logs	Indefinitely	Hard copy
Asbestos logs	Indefinitely	Electronic
First aid / incident reports	5 years	Hard copy
Installation of building systems	5 years / as long as the system is in use – see building file	Hard copy
Fire drill reports		Hard copy
Financial records	Current year plus six previous years	Electronic
Payroll records	Current year plus six previous years	Electronic
Customer records	As long as needed	Electronic
HR files	6 years	Hard copy
Job applications from unsuccessful candidates	6 months	Hard copy and / or electronic
Volunteer records	1 year	Hard copy and / or electronic