Breakthrough Data Protection Policy

Approved by Lead Organisation: November 2017
Next Review Date: November 2018

Introduction

The Partner organisations within the Breakthrough Programme need to collect and use certain types of information about the Data Subjects who come into contact with it in order to carry on our work. This personal information must be collected and dealt with appropriately– whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this under the Data Protection Act 1998.

This policy should be read in conjunction with the local Email and Internet Policy and the Safeguarding Policy.

Why this Policy exists

This Data Protection Policy ensures the programme:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individual's data.
- Protects itself from the risks of a data breach.

Data Protection Law

The Data Protection Act 1998 describes how organisations; including the Breakthrough programme partnership must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA) unless that country or territory also ensures an adequate level of protection

The partnership will, through appropriate management,

- Observe fully conditions regarding the fair collection and use of information,
- Meet its legal obligations to specify the purposes for which information is used,
- 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,
- Ensure the quality of information used,
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken,
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information),
- Take appropriate technical and organisational security measures to safeguard personal information,
- Ensure that personal information is not transferred abroad without suitable safeguards,
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- Set out clear procedures for responding to requests for information.

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

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) 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 the partnership (for example: a client, an employee, 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. Explicit consent is needed for processing sensitive* data

***** See definition

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. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within the partnership.

**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

People, risks and responsibilities

Policy scope

This policy applies to:

- The lead organisation for the Breakthrough programme
- All partners within the programme
- All staff and volunteers working on the Breakthrough programme
- All contractors, suppliers and other people working on behalf of partners in delivering Breakthrough

It applies to all data that the company holds relating to identifiable individuals, even if that information technical falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect all stakeholders in the Breakthrough programme from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with the Breakthrough programme has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

- The **Board of Trustees** for BRANCAB as the lead organisation is ultimately responsible for ensuring that Breakthrough meets its legal obligations.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work.**

- Data **should not be shared informally.** When access to confidential information is required, employees can request it from their line manager.

- **Partners will provide training** to all employees to help them understand their responsibilities when handling data.

- Employees should keep all data secure and in accordance to local Information Security Policy.

- Personal data **should only be disclosed** in accordance to local Information Sharing/Disclosure Policy.

- Employees **should request help** from their line manager or the Programme Management Team should they need further advice.

Disclosure

The lead organisation may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows the partnership to disclose data (including sensitive data) without the data subject's consent.

These are:

1. Carrying out a legal duty or as authorised by the Secretary of State
2. Protecting vital interests of a Data Subject or other person
3. The Data Subject has already made the information public
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion
6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

Data collection
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.

Partners will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, by completing a form, over a telephone, from a website or third party supplier..
When collecting data, Partners will ensure that the Data Subject:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- 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

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

When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

It is the responsibility of all partners 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.

Data access and accuracy
All Data Subjects have the right to access the information the programme holds about them. Partners will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, partners will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection,
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice,
- Everyone processing personal information is appropriately trained to do so,

- Everyone processing personal information is appropriately supervised,
- Anybody wanting to make enquiries about handling personal information knows what to do,
- It deals promptly and courteously with any enquiries about handling personal information,
- It describes clearly how it handles personal information,
- It will regularly review and audit the ways it hold, manage and use personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are 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 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.

Compliance

Failure to adhere to this policy could lead to disciplinary action.

In case of any queries or questions in relation to this policy please contact the Breakthrough Programme Management Team.