BEING THE CURE

DATA PROTECTION POLICY

APPROVED BY: Finance, Strategy and Risk Committee
APPROVED ON: 01/08/2024
NEXT REVIEW: 01/08/2025

Registered Charity 1188077
67 Central Park Road
London, E6 3DW
020 3443 9782

Info@beingthecure.org
www.beingthecure.org

CONTENTS

1. AIMS

Being The Cure aims to ensure that all personal data collected about staff, pupils, parents, trustees, volunteers, visitors, and other individuals is collected, stored, and processed in accordance with UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of the:

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

3. DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: Name (including initials) Identification number Location data Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Term	Definition
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. THE DATA CONTROLLER

Being The Cure processes personal data relating to staff, pupils, parents, trustees, volunteers, visitors, and others, and therefore is a data controller.

The charity is registered with the ICO has paid its data protection fee to the ICO, as legally required.

5. ROLES AND RESPONSIBILITIES

This policy applies to **all staff, trustees and volunteers** and to external organisations or individuals working on our behalf. For the purposes of this policy, the term ***colleagues*** will be used to refer to all of these groups collective. Colleagues who do not comply with this policy may face disciplinary action.

5.1 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring the charity's compliance with

data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on data protection issues.

The DPO is also the first point of contact for individuals whose data the charity processes, and for the ICO. Due to the size of the charity, the CEO assumes the role of the DPO until a DPO is hired for the charity.

5.2 CEO

The CEO acts as the representative of the data controller on a day-to-day basis.

5.3 The Board of Trustees

The board has overall responsibility for ensuring that Being the Cure's DPO complies with all relevant data protection obligations.

5.4 Colleagues

Colleagues are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach

- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties.

6. DATA PROTECTION PRINCIPLES

The UK GDPR and Data Protection 2018 are based on data protection principles that Being The Cure must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how Being The Cure aims to comply with these principles.

7. COLLECTING PERSONAL DATA

7.1 Lawfulness, fairness, and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Being The Cure can **fulfil a contract** with the individual, or the individual has asked Being the Cure to take specific steps before entering into a contract
- The data needs to be processed so that Being The Cure can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual or another person i.e., to protect someone's life

- The data needs to be processed for the **legitimate interests** of Being The Cure or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation, and accuracy

We will only collect personal data for specified, explicit, and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. The DPO will create relevant Data Impact Assessments (DIAs) for the personal data collected as part of all key delivery and operational activities of the charity.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Colleagues must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when colleagues no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with Being the Cure's record retention schedule within the data protection register or the appropriate DIA.

8. SHARING PERSONAL DATA

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our colleagues at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this

Our suppliers or contractors may need data to enable us to provide services to our colleagues and pupils – for example IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so (for example for safeguarding issues).

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or colleagues.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that Being The Cure holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address

- Details of the information requested

If colleagues receive a subject access request in any form, they must immediately forward it to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)

- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymize, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time

- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If colleagues receive such a request, they must immediately forward it to the DPO.

10. PHOTOGRAPHS AND VIDEOS

As part of our activities, we may take photographs and record images of individuals. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing, and promotional materials. This process will be undertaken before we begin working with a new cohort of children.

Any photographs and videos taken by parents/carers at events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where Being The Cure takes photographs and videos, uses may include:

- Within our own brochures, newsletters, promotional printed materials etc.
- Online on our website or social media pages
- As part of our press packs for local and national media channels

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

11. DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments for Being the Cure's processing of personal data key activities, new projects and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training colleagues on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

12. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left anywhere where there is general access.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

13. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely

dispose of records on our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

14. PERSONAL DATA BREACHES

Being The Cure will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of personal data through hacking or other data stealing methods online
- Accidental sharing of personal data outside of the organisation.

15. TRAINING

Colleagues are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Being the Cure's processes make it necessary.

16. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

On finding or causing a breach, or potential breach, the colleague or data processor must immediately notify the data protection officer (DPO) by email, listing the date and nature of the breach.

The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Colleagues will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the CEO and board of trustees

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant colleagues or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g., from IT providers).

The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences

The DPO will establish whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on Teams, in the data protection policy folder

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of awareness of the breach. As required, the DPO will set out:

A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the charity's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

Where Being The Cure is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on Teams, within the relevant data protection policy folder

The DPO and CEO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

The DPO and CEO will meet annually to assess recorded data breaches and identify any trends or patterns requiring action by Being the Cure to reduce risks of future breaches.

PERSONAL DATA BREACH PROCEDURE

Below are suggested response plans to some of the common types of data breach that the organisation might experience:

Phishing attacks

Attackers use deceptive emails or messages to trick employees or volunteers into revealing sensitive information such as login credentials or financial details.

Response Plan:

1. **Identify**: Confirm the phishing attack and gather information on the scope and potential data compromised.
2. **Contain**:
    - Isolate affected accounts.
    - Block malicious IPs and URLs.
3. **Eradicate**:
    - Remove phishing emails from all inboxes.
    - Update email filtering rules.
4. **Recover**:
    - Reset passwords for affected accounts.
    - Reinforce MFA where applicable.
5. **Notify**: Inform affected individuals and stakeholders about the breach and steps taken.
6. **Review**: Conduct a post-incident review to improve training and technical measures.

Ransomware

Malware that encrypts the organization's data and demands a ransom for the decryption key.

Response Plan:

1. **Identify**: Confirm the ransomware attack and determine the affected systems.
2. **Contain**:
    - Disconnect infected devices from the network.
    - Stop further encryption if possible.
3. **Eradicate**:
    - Remove the ransomware from infected systems using antivirus/anti-malware tools.
4. **Recover**:
    - Restore data from clean backups.
    - Rebuild affected systems if necessary.
5. **Notify**: Report the incident to law enforcement and inform affected parties.
6. **Review**: Analyse the breach to improve backup practices and security measures.

Data theft from physical devices

Theft or loss of physical devices such as laptops, smartphones, or USB drives containing sensitive data.

Response Plan:

1. **Identify**: Confirm the theft or loss of the device and assess the data at risk.
2. **Contain**:
    - Activate remote wipe if possible.
    - Lock accounts accessed by the stolen device.
3. **Eradicate**:

- Ensure device is no longer connected to the network.
- Change all credentials potentially accessed via the device.

4. **Recover**:
    - Restore data from backups to new devices.
    - Enhance physical security measures.
5. **Notify**: Notify affected individuals and authorities if required by law.
6. **Review**: Improve device encryption and physical security protocols.

Accidental data sharing outside the organisation

Accidental data breaches occur when sensitive information is unintentionally shared outside the organisation, often due to human error or miscommunication.

Response Plan:

1. **Identify**:
    - Determine what data was shared, how, and to whom.
2. **Contain**:
    - Attempt to recall the message or restrict access.
    - Contact the recipient to request deletion.
3. **Eradicate**:
    - Confirm with recipients that data is deleted.
    - Ensure future communications use secure channels.
4. **Recover**:
    - Assess any further actions needed.
    - Notify affected individuals and authorities if required.
5. **Notify**:

- Inform internal stakeholders.
- Notify affected parties and regulatory bodies if necessary.

6. Review:
    - Conduct a post-incident review.
    - Update policies and provide additional training.
    - Implement data loss prevention tools.