



**Brent Centre
for Young People**
healthy minds, brighter futures.

Clinical Data Protection Policy

Last reviewed: October 2025

Next review: October 2027

If you suspect there has been a data breach, immediately

contact the following people - if a breach meets the threshold for reporting the Data Protection Officer must inform the ICO within 72 hours

- Data Protection Officer (dataprotection@brentcentre.org.uk)

Inform them what personal data you think has or may have been compromised, how this happened, and which person or people may be affected.

What is a personal data breach? (from <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/>)

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Example (for more examples, see: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breach-examples/>)

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

1. Introduction

The Brent Centre for Young People (hereafter referred to as 'BCYP' or 'the Charity') is committed to protecting the confidentiality and security of clinical data. This policy outlines the principles and procedures we follow to ensure the protection of patient information in accordance with UK data protection laws, including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

As part of the services we offer, we are required to process personal data about our service users and, in some instances, the carers or relatives of our service users. "Processing" can mean collecting, recording, organising, storing, sharing or destroying data. We are committed to being transparent about why we need your

personal data and what we do with it. This information is set out in this privacy notice. It also explains your rights when it comes to your data. We will do our very best to look after your personal information. We want everyone who comes to us for support to feel confident about how any personal information they give will be handled, used and secured.

You can be confident that:

- We will never release your information to organisations outside BCYP for their marketing purposes;
- We only use personal information in the ways we need to and that is expected of us;
- We will be especially careful and sensitive when engaging with vulnerable people or those we have reason to believe might be vulnerable;
- We take all reasonable care to safeguard your personal information through security policies and secure business processes;
- We will always provide easy ways for you to contact us. Our Data Protection Officer (DPO) is happy to answer any queries you may have, contact details for our DPO can be found at the end of this policy.

2. Purpose

The purpose of this policy is to:

- Ensure compliance with legal and regulatory requirements.
- Protect the rights and privacy of patients.
- Maintain the integrity and security of clinical data.
- Promote a culture of data protection within the Charity.

3. Scope

This policy applies to all staff, volunteers, contractors, and third parties who handle clinical data on behalf of the BCYP. It covers all forms of data, including electronic, paper, and spoken information.

4. Definitions

- **Clinical Data:** Any information relating to a patient's health, treatment, or care, or any information which is personally identifiable
- **Data Subject:** An individual whose personal data is processed.
- **Data Controller:** BCYP, which determines the purposes and means of processing personal data.
- **Data Processor:** Any entity that processes personal data on behalf of the Data Controller.

5. Legal Framework

This policy is based on the following legal frameworks:

- General Data Protection Regulation (GDPR)

- Data Protection Act 2018
- NHS Data Security and Protection Toolkit (where applicable)
- BCYP's Confidentiality policy

6. Principles

The BCYP adheres to the following data protection principles:

1. **Lawfulness, Fairness, and Transparency:**
 - Process personal data lawfully, fairly, and in a transparent manner.
 - Provide clear information about how clinical data is used.
2. **Purpose Limitation:**
 - Collect data for specified, explicit, and legitimate purposes.
 - Do not process data in a manner incompatible with those purposes.
3. **Data Minimisation:**
 - Ensure data collected is adequate, relevant, and limited to what is necessary.
4. **Accuracy:**
 - Keep data accurate and up to date.
 - Correct or delete inaccurate data without delay.
5. **Storage Limitation:**
 - Retain data only for as long as necessary.
 - Follow retention schedules and secure deletion protocols.
6. **Integrity and Confidentiality:**
 - Protect data against unauthorised or unlawful processing, accidental loss, destruction, or damage.
 - Implement appropriate technical and organisational measures.
7. **Accountability:**
 - Demonstrate compliance with data protection principles.
 - Maintain records of processing activities.

7. Data Subject Rights

The BCYP respects and upholds the rights of data subjects, including:

- **Right to Access:** Patients can access their personal data and obtain information about its processing. This does not apply to clinical session notes. Patients can request access to clinical session notes under certain circumstances, please refer to our Subject Access Request. If a court order demands access to patient notes the BCYP will comply within the correct legal framework.
- **Your right to rectification** - You have the right to ask us to correct any data we have which you believe to be inaccurate or incomplete. You can also request that we restrict all processing of your data while we consider your rectification request;
- **Your right to erasure** - You have the right to ask that we erase any of your personal data which is no longer necessary for the purpose we originally collected it for. We retain our data in line with the Data Protection

- **Your right to restriction of processing** - You may also request that we restrict processing if we no longer require your personal data for the purpose we originally collected it for, but you do not wish for it to be erased.
- **Your right to object to processing** - If we are processing your data as part of our legitimate interests as an organisation or to complete a task in the public interest, you have the right to object to that processing. We will restrict all processing of this data while we investigate your objection.

If you make any of the above requests, we may ask you to provide proof of identity. This is to make sure that data is not shared with the wrong person inappropriately. We will always respond to your request as soon as possible and at the latest within one month. You are not required to pay any charge for exercising your rights.

Please contact us at dataprotection@brentcentre.org.uk if you wish to make a request.

If you would like to complain about how we have dealt with your request, please contact: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF (<https://ico.org.uk/global/contact-us/>).=

8. Processing of Service User Data

BCYP may collect personal information from you when you interact with us, for example: if you enquire about our activities, make a referral to us, during treatment, if you make a donation to us, if you choose to provide us with optional feedback, or otherwise provide us with personal information. We may collect this information over the phone, via our website, through the post, or in person.

What data we collect:

So that we can provide a safe and professional service, we need to keep certain records about you. We may process the following types of data under Article 6.1(f) of the General Data Protection Regulation:

- Your basic details and contact information e.g. your name, address, date of birth, postal address, telephone number;

We also collect the following data, which is classified as “special category”, under Article 9.2(h) of the General Data Protection Regulation:

- Health and social care data about you, which might include both your physical and mental health data;
- We may process data about your race, ethnicity, sexual orientation, disability, or religion/spiritual/philosophical beliefs.

Where this data is collected via survey rather than during treatment, it will not be processed onwards unless in unidentified form. This means in a format where your identity and privacy are protected.

How do we use personal information?

We may use your personal information to:

- Provide you with the important advice and support you've asked us for;
- Provide or administer activities relating to all our services: updating you with important administrative messages, to help us identify you when you contact us, and help us to properly maintain our records;
- Audit and report on our service delivery;
- Research or archiving purposes: We use the information collected to conduct research to better understand the mental health needs of our patients and the effectiveness of our services. Any information used in this way will always be anonymised. This allows us to improve and adapt our services, and to understand if new services or other types of support would be appropriate to meet changing needs;
- Improve your experience with us. We may use your information to enhance the service that our staff provide and improve our information and communication.

A special note about the Special Category Information we hold:

We only use this information for the purposes of dealing with your enquiry, treatment provision, training, quality monitoring, audit and evaluation of the services we provide. We will not pass on your identifiable details to anyone else without your knowledge except in exceptional circumstances.

If you provide us with any such information by telephone, email or by other means, we will treat the information with extra care and always in accordance with BCYP's Privacy Policy.

Your personal information and details of the enquiries received are stored on a secure database. They will be kept for the duration of your treatment. For adult service users, data will be kept for 8 years after the end of treatment; for under 18s, records will be kept until the age of 25 (or until the age of 26 if the young person is aged 17 when treatment ends). If this information is kept for longer, in exceptional circumstances, we will inform you of this.

Who sees your personal information?

The personal information we collect about you will be used by our staff and approved volunteers in BCYP so that they can support you. We will routinely share information with your GP/health service to ensure joined up care, this does not include confidential session material which is subject to BCYP's confidentiality policy.

In exceptional circumstances (not routinely unless with consent) and to the best of our ability with the knowledge of the individual/s concerned, we may share information with parents/guardians, particularly if there are safeguarding concerns, please refer to BCYP's confidentiality policy and safeguarding policy for more details.

We will never sell or share your personal information with organisations so that they can contact you for any marketing activities.

We may share data with the NHS or other healthcare partners, but this will always be in an anonymous format. Anonymous clinical care data may be re-used, including through linkage with other data sources, for the purpose of data analysis and reporting.

9. Data Security

BCYP implements the following security measures:

- **Access Controls:** Limit access to clinical data to authorised personnel only.
- **Encryption:** Use encryption to protect data in transit and at rest.
- **Regular Audits:** Conduct regular security audits and risk assessments.
- **Incident Management:** Establish procedures for reporting, managing, and responding to data breaches.

10. Data Sharing

- **Third-Party Processors:** Ensure third parties processing data on behalf of the Charity comply with data protection laws and contractual obligations.
- **Data Sharing Agreements:** Use data sharing agreements to govern the sharing of clinical data with other organisations.
- **Patient Consent:** Obtain consent (verbal or written) from patients before sharing their data, unless otherwise required by law or for safeguarding reasons.

11. Retention and Disposal

- **Retention Schedule:** Follow a documented retention schedule for clinical data.
- **Secure Disposal:** Ensure secure disposal of data that is no longer required, using methods such as shredding, degaussing, or secure digital deletion.

12. Monitoring and Review

- **Policy Review:** Review this policy annually or in response to changes in legislation or organisational practices.
- **Compliance Monitoring:** Monitor compliance with this policy and take corrective action as needed.

13. Breach Notification

- **Internal Reporting:** Report data breaches immediately to the Data Protection Officer (DPO).
- **Regulatory Reporting:** Notify the Information Commissioner's Office (ICO) within 72 hours of a breach, where required.
- **Patient Notification:** Inform affected patients of data breaches when there is a high risk to their rights and freedoms.

14. Responsibilities

- **Data Protection Officer (DPO):** Oversee data protection strategy and implementation.
- **Management:** Ensure staff compliance with this policy.
- **Staff and Volunteers:** Follow this policy and attend required training.

15. Contact Information

For any questions or concerns regarding this policy, contact the Data Protection Officer at:

Jameel Ukaye, Data Protection Officer
The Brent Centre for Young People
51 Winchester Avenue, London, NW6 7TT
Phone: 020 7328 0918
Email: dataprotection@brentcentre.org.uk

This policy ensures that BCYP handles clinical data responsibly, ethically, and in compliance with legal standards, safeguarding the trust and privacy of our patients.