Brainkind

Data Protection Policy

Ver4.0 September 2022

26.09.2022

Author: Data Protection Officer

Document type:	Policy Name
Version:	4.0
Primary Sponsor:	Legal and Corporate Compliance
Co-Sponsors:	-
Approved by:	Policy Review Group
Date Policy Implemented:	26/09/2022
Policy Review Date:	26/08/2025 (30 days before expiry)
Policy Expiry Date:	26/09/2025
Date uploaded to Portal:	05/10/2022
Review Frequency:	3 Years

Version	Date	Type of change	Revisions since previous
Ver 4.0	26/09/22	Major update	Policy Redrafted

Contents

1 Introduction 3

2 Purpose/Scope 3

3 Key Definitions 3

4 Roles and Responsibilities and Compliance 4

5 Principles and Guidance 5

6 Approaches and Procedures 7

7 Security of Personal and Confidential Data 10

8 Training for Staff 12

9 Related Policies 12

Appendix A: Safe Haven Principles (Guidance on the Secure Transfer of Confidential Information) 13

1 Introduction

Brainkind collects, uses, stores, and otherwise processes personal data relating to staff, the people we support, and others in the course of its operation. Additionally, staff have a duty of confidentiality to the people we support. Brainkind is committed to protecting such personal data and maintaining confidentiality in accordance with the applicable laws and guidance.

2 Purpose/Scope

This policy sets out how Brainkind manages its data protection and confidentiality obligations. It applies to, and must be read and understood by, everyone working for or acting on behalf of Brainkind, including all permanent and temporary staff, contractors, students and researchers.

Questions regarding this policy can be directed to the Data Protection Officer. Any incident involving a breach or suspected breach of this policy must be reported immediately via the Datix incident reporting system at Datix: Brainkind Incident Reporting Form (DIF1) - V4 Sept 2021 (datixsolutions.co.uk)

Failure to comply with this policy may result in Brainkind facing prosecution, including a financial penalty, and disciplinary action being taken against individuals.

3 Key Definitions

Personal data is any information relating to an identified or identifiable individual, including a name, photo, email address, and medical information.

Some types of personal data are likely to be more sensitive and therefore benefit from additional legal protection; these are referred to as **special category data**. This includes information revealing an individual's racial or ethnic origin, political opinions or religious beliefs; genetic and biometric information such as fingerprints or facial recognition data; and information about a person's sex life or sexual orientation or relating to criminal allegations, convictions or offences.

Processing personal data entails any operation performed on the data, including collection, recording, organising, storing, using, altering, retrieving, consulting, disclosing or otherwise making available, combining, erasing or destroying.

4 Roles and Responsibilities and Compliance

The Board of Trustees, specifically the Quality and Governance Committee, and the Chief Executive have overall responsibility for lawful data protection and confidentiality compliance. The Board will monitor compliance through receipt of quarterly reports. **The Information Risk Management Group** will monitor operational progress and take action to address any concerns.

The **Data Protection Officer** is responsible for day-to-day data protection matters, including:

- Informing and advising Brainkind on data protection obligations and enquiries.
- Providing advice regarding Data Protection Impact Assessments (DPIAs).
- Serving as a point of contact with the data protection regulatory authority.
- Handling complaints and appeals regarding Brainkind's data protection policies and procedures.

The Director of Digital, in their capacity as **Senior Information Risk Officer (SIRO)**, is responsible for development of appropriate policy and procedure and for ensuring any suspected or actual data breach is handled appropriately.

Information Asset Owners (IAOs) and **all line managers** are responsible for ensuring that their employees are compliant with the relevant data protection policies and procedures, as well as championing good information-handling practices within Brainkind. IAOs are also responsible for ensuring that all individuals who have authorised access to personal data are subject to an appropriate confidentiality agreement.

5 Principles and Guidance

We must be guided by certain principles from the law and appropriate guidance when processing personal data and handling confidential information. All staff are expected to adhere to these principles.

5.1 Principles from Data Protection Legislation

Brainkind is responsible for, and must be able to demonstrate compliance with, the following principles from data protection legislation:

a) fairness and transparency: Brainkind must process personal data legally and fairly, and provide the individual that the personal data relates to with information about why and how their personal data is processed;

b) purpose limitation: Brainkind shall only collect personal data for a specific, explicit and legitimate purpose. Any subsequent processing must be compatible with the purpose for which the data was collected, unless Brainkind has obtained the individual's consent to the new use or the processing is otherwise permitted by law;

c) data minimisation: Brainkind shall only process personal data that is adequate, relevant and limited to what is necessary for the purposes for which it was collected;

d) data accuracy: Brainkind shall ensure that personal data is accurate and complete, and take reasonable steps to ensure it is kept up-to-date;

e) individual rights: Brainkind shall allow individuals to exercise their legal rights in relation to their personal data;

f) storage limitation: Brainkind shall only keep personal data for as long as it is needed, for the purposes for which it was collected or for a further permitted purpose; and

g) data security: Brainkind shall use appropriate security measures to protect personal data, including where third parties are processing personal data on its behalf.

5.2 The Caldicott Principles

Brainkind must also adhere to the Caldicott Principles, which are principles created for all NHS organisations to follow when handling and using “patient-identifiable information”, namely the individual’s name, date of birth, address, image and other recordings of them, their NHS number and local codes, and anything else that could be used to identify them directly or indirectly, such as rare diseases, drug treatments, or statistical analyses using small sample sizes.

In summary, the Caldicott Principles are:

- to always be able to justify the purpose of using or transferring patient-identifiable information and to only do so lawfully;
- to only use identifiable information where absolutely necessary;
- to use the minimum identifiable information necessary;
- to restrict access to identifiable information to only those that need it;
- to inform individuals about how their confidential information is used and what choices they have over this, which as a minimum means providing accessible, relevant and appropriate information;
- that everyone should be aware of their responsibilities and obligations with respect to identifiable information; and
- that the duty to share information where it is in the best interests of the people we support can be as important as the duty to protect confidentiality, and staff should have confidence to do so using the appropriate procedures.

5.3 The Safe Haven Principles

Brainkind also adheres to the Safe Haven principles regarding the secure storage and external transfer of confidential data. All staff handling confidential information relating to the people we support and/or staff, whether paper based or digital, must adhere to these principles.

Please see Appendix A and speak to the Data Protection Officer for more information.

6 Approaches and Procedures

6.1 Lawful Processing

Whenever Brainkind processes personal data, we must have a legal basis to do so. The legal bases available are set out in data protection law. In summary, they are:

- **consent:** the individual that the personal data is about has consented to the processing;
- **contractual necessity:** the personal data must be processed in order to carry out a contract with the person that the personal data is about, or take steps at their request before entering into a contract;
- **public interest:** the processing of personal data is necessary to perform a task in the public interest or in the exercise of an official authority;
- **compliance with legal obligations:** the processing of personal data is necessary to comply with the law;
- **legitimate interest:** the processing of personal data is necessary for the purposes of a legitimate interest; and
- **vital interests:** the processing of personal data is necessary to protect the vital interests of the person the data is about or of another person.

Each legal basis has specific conditions and caveats for when it can be used. For more information, speak to the Data Protection Officer.

Note that Brainkind should not use consent as the legal basis of processing personal data for its core activities because, given the nature of our work, it is unlikely that consent could be deemed to be freely given. Instead, contractual necessity and public interest are likely to be the main legal bases we rely on for processing, for which the relevant part of the contract or the official authority that the processing is necessary to carry out will need to be identified.

6.2 Individuals' Rights

Staff, the people we support, and others have rights regarding how we handle their personal data, including, where certain conditions are met, the right to:

1. be informed about how Brainkind collects and uses their personal data;

2. ask for access to their personal data that Brainkind holds;

3. ask Brainkind to rectify inaccurate data or complete incomplete data;
4. ask Brainkind to erase their personal data;
5. limit the ways Brainkind can use and process their personal data;
6. object to the processing of their personal data,

as well as other rights in relation to automated decision making and profiling.

Brainkind must respond to a request from an individual regarding their rights without delay and within one month of receipt of the request.

If Brainkind decides not to take action on a request, Brainkind must still respond to provide an explanation to the individual and inform them of their right to complain to the Information Commissioner's Office and to a judicial remedy.

6.3 Complaints and Enquiries

Complaints about Brainkind's data protection procedures and appeals against decisions not to supply exempt information will be dealt with by the Data Protection Officer, who will handle the complaint in accordance with Brainkind's Complaints Policy.

The Data Protection Officer will also handle general enquiries and provide advice to Trust departments about data protection legislation.

6.4 Data Protection Impact Assessments (DPIAs)

Brainkind must carry out a documented Data Protection Impact Assessment (DPIA) before commencing any new project or initiative that involves processing of personal data that is likely to result in a high risk to the rights and freedoms of individuals. The DPIA will be used to help Brainkind identify and minimise the data protection risks with the proposed processing.

Brainkind's Data Protection Impact Assessment Policy can be found on Policy Manager at Connect - Policy details (myintranet.com). More information can be found in the DPIA Policy.

6.5 Record of Processing Activity

Brainkind must maintain an up-to-date documented record of its processing activities. It shall be the responsibility of the Director of Digital to maintain the record.

6.6 Privacy by Default

Any new processing activity or functionality involved in the processing of personal data should be designed and used with the approach of “privacy by default”, which means that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of the processing, the period for which the personal data is stored and its accessibility.

6.7 6.7 Information Sharing and Use of Service Providers

Brainkind is currently a signatory to a number of regional information-sharing protocols and agreements for the exchange of personal data between health and social care organisations and other partner agencies/companies. These protocols and agreements do not in themselves render the exchange lawful: compliance with this policy is still required. Brainkind will ensure it is proactive in putting specific information sharing agreements in place when required.

If Brainkind uses a third party to process personal data on its behalf (for example, IT hosting or email marketing), Brainkind is legally required to have a written contract with the service provider which imposes some specific obligations on the service provider. For more guidance on this, consult the Data Protection Officer.

6.8 Research

Personal data collected for the purposes of research is subject to data protection legislation, although there are exemptions for processing in particular circumstances. Speak to the Data Protection Officer for more information.

Personal data processed solely for research purposes benefits from certain exemptions from data protection legislation if:

- the data are not processed to support measures or decisions with respect to particular individuals; and
- the individuals the data relate to are not caused substantial harm or distress by the processing of the data.
- If the above conditions are met, then personal data processed for research purposes only:
- can be processed for purposes other than that for which they were originally collected (although note that Brainkind still expects that wherever possible, researchers will contact participants if it is intended to use the data for purposes beyond those for which the data were originally collected);
- can be held by Brainkind indefinitely; and
- does not have to be disclosed as part of a request from an individual (see section 6.2) where the data are processed for research purposes and the results are anonymised.

Researchers must adhere to Brainkind's Records Management Policy. Researchers must ensure that the findings of research are anonymised when published and that no information is published that would allow individuals to be identified without their explicit consent. Further guidance on anonymisation can be found in the Information Commissioner's Office's Anonymisation Code of Practice.

7 Security of Personal and Confidential Data

To help ensure that personal and/or confidential data is protected to prevent theft, fraud and breaches of confidentiality and security, all staff must adhere to basic security principles, ensuring that:

- security practices are observed and carried out as part of their daily routine;
- computer passwords are not shared with other employees and computer workstations not left unattended and unsecure;
- all records containing confidential data are stored in secure areas with appropriate and adequate controls in place to hold and process it securely

i.e. in a lockable room with controlled access or in a locked drawer or filing cabinet;

- information published to online and digital sources is fully anonymised and does not breach data protection legislation (refer to the Management of Online and Digital Services Procedure for mandated requirements).
- premises and vehicles are suitably secure so as not to put information assets (e.g. laptops or paper records containing confidential data) at risk;
- any swipe cards are not left unattended and cards and access PIN codes are not shared with other staff;
- confidential data is only used and shared with authorisation to do so and with organisations or individuals that are authorised to receive it;
- ID badges are worn at all times, where these are issued;
- the status of strangers is queried if safe to do so; and
- you inform your line manager if anything suspicious or worrying is noted.

Furthermore, regarding personal data and commercially sensitive data, all staff must ensure that:

- no such data is stored on personal computer devices. All equipment used for work purposes must be supplied by Brainkind, unless employees are using Brainkind's Outlook on the web server or NHSmail;
- such data transmitted via the internet or file transfer protocol is encrypted to 256 bit AES encryption;
- emails containing such data are only transmitted outside of Brainkind's own secure email network if the email or email transmission method is encrypted to 256 bit AES encryption. Refer to the Information Security Policy for mandated requirements;
- any such data held and transported on portable devices e.g. laptops, CD, DVD etc. has been approved in advance by Brainkind's Senior Information Risk Owner (SIRO) and is encrypted to 256 bit AES encryption; and

- there is a clear business need to use paper-based copies of documents containing such data off-site and adhere to safe haven principles (see Appendix A).

Brainkind does not support the use of fax machines for the routine transfer of personal data and its use should be avoided wherever possible. Where it is necessary and there is no secure alternative to transfer personal data on an ad hoc basis by fax, the safe haven principles and procedures must be followed. Please see Appendix A. Information Asset Owners are expected to take proactive steps to implement secure alternatives for the transfer of personal data.

8 Training for Staff

Training is delivered as specified within Brainkind Training Needs Analysis (TNA).

9 Related Policies

All employees must adhere to the following related policies:

- Subject Access Request Policy
- Information Security Policy
- Worker Digital Access Policy
- Website Policy and Procedure
- Records Management Policy
- Mobile Devices Policy
- Social Media Policy
- Physical Security Policy
- Clear Desk and Screen Policy

Appendix A: Safe Haven Principles (Guidance on the Secure Transfer of Confidential Information)

This guidance applies to all records in whatever media they may be held (e.g. paper, electronic files and emails, images and audio recordings), which include confidential data relating to the people we support, employees or others.

Internal and External Post

- Ensure envelopes containing confidential information are sealed and marked ‘private and confidential’.
- Double check the full postal address (including postcode) of the recipient is correct.
- Ensure internal mail has been addressed fully and correctly, providing at least the following basic information;
  - First Name and Surname – Jane Doe
  - Department - Finance Department
  - Site – Burgess Hill
- If addresses are handwritten please make them legible for the post room staff.
- Cross out the previous address on internal envelopes to stop any confusion on the next recipient.
- Use two envelopes for bulky letters for extra security.
- Take care when using window envelopes that the correct, full address is visible. No other information should be visible.
- Use only the correct, sealed record bags and wallets for transferring service user care records via Brainkinds internal transport service to Healthcare Records. Service user care records must not be placed in the internal or external post to transfer them to Healthcare Records.

- Make sure that inbound post is handled promptly and securely around the workplace.

- Ensure you have a designated area within your Department or Service for mail collection and deposit. In the absence of defined lockable and managed post rooms at most Trust sites, any inbound or outbound mail (this includes employee payslips) which is to be left uncollected and unattended at a Service or at any Disabilities Trust site, for any length of time, should be locked away in a specially designated locked drawer or locked filing cabinet or within an office which is kept locked when not in use, ideally within the Service Manager's office. Existing pigeon hole systems can be used if they are within an internal locked office.

- Routine transfers of personal data or special categories of data by internal or external post must be recorded on your departmental data flow records.

Royal Mail Special Delivery and Courier Services (full tracked services)

- Seek advice from your line manager or the Information Governance Officer on whether Royal Mail Special Delivery or other approved courier service should be used for ad hoc transfers of confidential information externally.

- Due to the added cost of sending items of post by Royal Mail Special Delivery or approved courier service, a risk assessment should be undertaken which considers the sensitivity of the information and number of identifiable individuals whose information is recorded.

- Computer media containing confidential information must not be transferred unless it is an encrypted copy of the original. It should only be transferred by Royal Mail Special Delivery or approved courier service. There are also additional requirements around removable media and bulk transfers (see below).

- Let the recipient know when to expect receipt of the item and ask the recipient to confirm receipt. The above principles relating to internal and external post also apply when using Royal Mail Special Delivery or approved courier services.

- Routine transfers of personal data or special categories of data by Royal Mail Special Delivery or approved courier must be recorded on your departmental data flow records.

Bulk Transfers

- Bulk transfers of personal data or special categories of data must have the approval of the relevant Information Asset Owner (IAO).
- When transferring bulk personal information you must use an approved courier or secure mail method which can be tracked and is signed for e.g. Royal Mail Special Delivery.
- When transferring personal information by approved courier:

  a) The individual responsible for passing the information to the courier must check the ID of the courier and obtain a receipt from the courier when the bulk personal information is collected.

  b) The sender must confirm the bulk transfer has been received by contacting the recipient.

  c) The courier must only hand this information over to the recipient or to a nominated individual and obtain a signature when delivered.

Removable Media

- The use of removable media such as CDs and DVDs for the writing of personal data or special categories of data, is prohibited other than for the approved transfer of large volumes of data where an alternative secure means of transfer (e.g. secure file transfer protocol or NHS Mail) is not feasible.

- Electronic personal information to be sent via removable media by post or courier must be encrypted to 256 bit AES encryption prior to transfer, in line with Department of Health encryption requirements. The transfer must be approved by Brainkind's Senior Information Risk Owner (SIRO).

- Information held on the removable media device must be securely erased or disposed of once the transfer is complete.

Pigeon-holes/In trays for paper information

- Regular housekeeping must be carried out in areas where pigeon-holes or in-trays are used to disseminate corporate and person identifiable information.

- Nothing should be left in these areas overnight especially in relation to sensitive information unless the area is secured.

Use of the Telephone

- Personal information must only be given over the telephone if you are confident of the identity of the caller. If you are not, you must always take a number, verify it independently and call back. When speaking to a service user or carer on the telephone, confirm the caller's identity or ring back.

- Always check whether an individual is entitled to the information they request. Information relating to the people we support must only be released on a need-to- know basis.

- If you receive suspicious queries asking the whereabouts, base or personal information of other employees, please treat with caution, take contact details of the caller and verify that it is an authorised person and request.

- Report any suspected bogus enquires to your line manager and as an incident on the Datix system.

- Messages about named the people we support must not be left on answerphones. Simply leave your name and telephone number and no other information.

- Ensure unauthorised people cannot overhear you when making sensitive telephone calls, during meetings, and when you are having informal discussions with colleagues about personal/business sensitive information. In these situations, if you do not need to identify an individual we support or employee by name, then don't.

Transcribing of telephone messages

- Recorded telephone messages containing person identifiable information including sensitive information such as the names and addresses of applicants telephoning for a job application, or an individual we support's details must be received into a secure location, so that only those entitled to listen to the message may do so whilst it is being played back.

- If you use any kind of message book e.g. to note messages for absent employees, this should also be stored securely.

Fax Transmission

- Fax is inherently insecure and is not recommended for transfer of personal information.

- Fax machines should only be used to transfer identifiable information relating to the people we support or staff-identifiable information where it is absolutely necessary to do so and there is no secure alternative.

- Always use a fax cover sheet to enforce the confidentiality of the message.

- Telephone the recipient of the fax (or their representative) to let them know you are sending them confidential information. Ask them to wait by the fax machine whilst you send your message through to them.

- Send a test fax transmission when sending to a new fax number.

- Send information to a Safe Haven fax whenever possible.

- Always double check the fax number before you hit the send button, whether the fax is Safe Haven or not.

- Use pre-installed numbers wherever possible to minimise the risk of dialling a wrong number.

- Request a report sheet that confirms your transmission has been successful.

- Ask the recipient to let you know when they receive the fax.

- Anonymise identifiable information relating to the people we support details wherever possible, but don't compromise service user safety.

Taking Paper Based Confidential Documents Off Site

- When working off-site the use of paper-based records containing identifiable information relating to the people we support or staff-identifiable information should be kept to a minimum. This also extends to any other information which Brainkind deems to be of a confidential and sensitive nature e.g. commercially sensitive information such as a tender document.

- There must be a clear requirement to take such information off-site in the first instance and when doing so, responsibility lies solely with you.

- Employees who have a clear business need to use paper-based copies of documents containing personal information off-site must adhere to the following:

    - Where the transfer is not an approved and acknowledged routine transfer for business purposes, make sure that your immediate line manager is aware that you have a requirement to take confidential information off-site and gain approval.

    - Keep equipment and paper-based records/files locked and out of sight during transit.

    - Keep usage to a minimum in public areas.

    - Ensure the security of information i.e. store it in a locked container (e.g. a filing cabinet, lockable briefcase). If this is not possible, when not in use, information should be neatly filed and stored away.

    - Do not dispose of any documents unless they can be shredded.

    - Ensure that the information is returned to Trust premises as soon as possible and filed accordingly.

    - Consider scanning the documents and then accessing them from a secure area via a Trust laptop or other suitable mobile device.

Mobile Computing

- All devices must be operated in a secure manner at all times.
- When not in use, devices should be kept in a secure place.
- Do not leave any device visible in an unattended vehicle.
- The amount of information that is kept on the device should be kept to a minimum.
- All information should be stored on Brainkind's servers where it is regularly backed- up.
- Details of any password or PIN must be kept secure.

Trust Laptops and Tablet Devices

Laptops and tablets left on display and unattended will inevitably attract attention and have the potential to be stolen. The security of your work laptop or tablet device is your responsibility. Please ensure that you adhere to the following:

- Ensure that your device is placed in a secure, locked location (e.g. desk drawer, filing cabinet) when not in use or left overnight on work premises.
- Ensure that your device is not left unattended in an insecure area where members of the public may have access (e.g. meeting rooms or hotel rooms). Always use lockable storage facilities where available.
- Be aware of opportunist or targeted thefts of laptop bags in busy public places, such as airports, train stations, hotel receptions and exhibition halls and on public transport.
- Ensure your device is stored securely and out-of-sight when travelling and not in use. When travelling by car, ensure your device is locked in the boot and never left on car seats or foot wells. Devices should be removed from cars if they are going to be left unattended for any length of time.
- Avoid leaving devices in locations where they could be easily forgotten or left behind e.g. overhead racks on trains or in the boot of a taxi.

Specifically, when working from home on your device:

- Ensure reasonable steps are taken to minimise visibility of your device from outside your home.
- Secure windows and doors when the home is unoccupied. Ensure blinds or curtains are closed.
- Make use of room locks and lockable storage facilities to secure your device.
- Where the option is available, always lock the device by pressing Control, Alt and Delete at the same time on your keypad and selecting the 'lock computer' option (alternatively press the Windows and 'L' keys together). This applies no matter how long you are leaving your device unattended for.
- Ensure that no other person e.g. family member of friends are allowed to access your device.
- Ensure that your device is connected to Brainkind's network at least once a month, to enable the automated update of antivirus software and other security features.
- On no account should you store any service user or staff-identifiable information on personal computer devices.

USB Devices

- If you require a memory stick (USB device) you must apply for an encrypted USB device that is approved by Brainkind. Please contact the ICT Service Desk via the self-service portal on Brainkind intranet Portal (myportallogin.com) and they will provide you with an application form. On collection, you will be given an instruction sheet and a password to unlock the device.
- If you have a requirement to take your USB device off-site, please ensure that you adhere to the following:
  - Whilst in transit, carry the device discretely in a closed container or bag and not on public view where it can attract attention.

- Store the device in a safe and secure environment when working off-site.
- Where practical, mark the device to identify its ownership by Brainkind.
- Be sure that an encrypted USB device is the most appropriate solution for storing work files. Make use of the secure drives and folders which enable you to share work across Brainkind's computer network.

Email

- Please refer to Brainkind's Email Policy for the mandatory and best practice requirements for the transfer of personal data, special categories of data and commercially sensitive information by email.
- Emails containing personal data, special categories of data and commercially sensitive information must only be transmitted to recipients outside of Brainkind's secure email network by using one of the three methods detailed below:-

    1. By use of NHS Mail (both the sender and the recipient of the email MUST be using NHS mail email addresses or email addresses that are part of the Government Secure Intranet). NHS Mail is also widely known as NHS.net email.

    2. By encryption (to 256 bit AES) of the information within a strongly password protected file attached to the email correspondence. Brainkind supports the use of WinZip for file encryption. Employees should contact the ICT Service Desk in relation to access to WinZip.

    3. By Secure File Transfer Protocol (SFTP)

- Strong passwords must be eight characters, alpha numeric, mixed upper and lower case.
- All transfers of person identifiable information, sensitive person identifiable information and commercially sensitive information outside of Brainkind's secure email network must be authorised by a Departmental Information Asset Owner or Head of Department