**Recruitment Data Privacy Policy**

**Does this notice apply to you?**

This privacy notice applies to all applicants that are not currently staff members of Brandon Trust. If you are applying for a promotion or another job in Brandon Trust and are already employed by Brandon Trust, please refer to the privacy notice for staff.

**Who are we?**

We are Brandon Trust. We provide support and services to enable people with learning disabilities and autism to live the lives they choose. In this policy, 'Brandon', 'we', 'us' or 'our' refers to Brandon Trust.

- We are a company registered in England and Wales: Number 2365487
- We are a registered charity in England and Wales: Number 801571
- We are registered as a data controller with the Information Commissioners Office: Registration Number Z1616504

**What is the purpose of this document?**

Brandon Trust is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during the application and recruitment process with us, in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, and any national laws, regulations and secondary legislation, as amended or updated from time to time, in the United Kingdom, and any other territory which implements the GDPR.

We, Brandon Trust are the Data Controller and responsible for maintaining security of any information you supply to us. We are required under data protection legislation to notify you of the information contained in this privacy notice.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

**Data protection principles**

We will comply with data protection law. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up-to-date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

**During the recruitment process, we may collect the following information from you:**

- Personal information that will include (but is not limited to) your name, title, address, including email address and telephone number, date of birth and gender.
- National insurance number.
- Next of kin and emergency contact information.
- Copy of driving licence.
- Employment history (including job titles) and education/qualification history (including professional memberships).
- We may also request further information to progress an application including but not limited to references, criminal and disciplinary history and right to work in the UK information, including passports, visas or national identity cards, and information contained in a CV or cover letter as part of the application process.
- If you contact us, we may keep a record of that correspondence (including email).

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity (only used for equal opportunities monitoring).
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

Please note, this data may be held either on Brandon networks and systems and/or on the iCIMS server, which is discussed further below.

We collect this information in a variety of ways from the application and recruitment process either directly from candidates or sometimes from an employment agency or background check provider. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment. We may sometimes collect additional information from third parties including former employers, or other background check agencies.

**Why do we need to process personal data?**

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to comply with a legal obligation, such as providing information to respond to requests from courts, law enforcement agencies and other public and government authorities.

- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests);

- Where it is needed in the public interest or for official purposes.

We need to process your personal data at your request to be able to carry out certain activities/tasks prior to entering into a contract with you. We also need to process your personal data to enter into a contract with you. In some cases, we need to process data to ensure that we comply with our legal obligations. For example, we are required to check a successful applicant's eligibility to work in the UK before they start working with us.

Situations in which we will use your personal information are as follows:

- Making a decision about your recruitment or appointment.
- Determining the terms on which you may work for us.
- Checking you are legally entitled to work in the work location in which you are to be based.
- Assessing qualifications for a particular job or task.
- Assessing education, training and development requirements.
- Dealing with legal disputes.
- Ascertaining your fitness to work.
- Complying with health and safety obligations.
- Preventing fraud.

- Facilitating equal opportunities monitoring.
- Keeping your details, with your consent, in case you are suitable for other positions with us.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

In some cases, we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests.

For example, we have a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide who to offer a job. We may also need to process data from job applicants to respond to and defend against legal claims.

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent. If we need your consent we will contact you separately about this.
- Where we need to carry out our legal obligations and in line with our data protection policy.
- Where it is needed in the public interest, such as for equal opportunities monitoring and in line with our data protection policy and equality and diversity policy.
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We process health information if we need to make reasonable adjustments to the recruitment process for candidates who have a disability, to ensure their health and safety, and to assesses their fitness to work. This is to carry out our obligations and exercise specific rights in relation to employment.

Where we process other special categories of data, such as information about ethnic origin and health, this is for equal opportunities monitoring purposes and to comply with employment and other laws, for example if you raise concerns which relates to a protected characteristic.

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of being successful in the application procedure with us that you agree to any request for consent from us.

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions. We will only collect information about criminal convictions if it is appropriate given the nature of the role applied for and where we are legally able to do so. For some roles, we are obliged to seek information about criminal convictions and offences. When we seek this information, we do so because it is necessary for us carry out our obligations and exercise specific rights in relation to employment. We will use information about criminal convictions and offences in the assessment for initial hiring.

**What do we do with your information?**

We may have to share your data with third parties including third party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

The system through which you apply for a job with Brandon is called iCIMS.

Please note the server currently used to store your job application information is based in the EU and is hosted by iCIMS, a third-party entity that is not a part of Brandon Trust. Please click here to view iCIMS privacy policy https://www.icims.co.uk/legal/privacy-notice-website/

iCIMS is responsible for the processing of personal data it receives, under EU & UK Law.

Your personal data will be shared internally for the purposes of the recruitment process. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles. Data will be stored in a range of different places including on your application record on iCIMS, on Brandon Trust networks/systems, HR Management Systems and on other IT systems (including email).

We will share your personal information with third parties where required by law, where it is necessary to administer the application process or where we have another legitimate interest in doing so.

"Third parties" includes third-party service providers (including contractors and designated agents). The following activities are carried out by third-party service providers: criminal records check from DBS and occupational health clearance from our provider. However, we will not pass on any information for any other purpose unless you authorise us to do so. We will also share your data with former employers for the purposes of obtaining references.

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Brandon Trust supports the objectives of the GDPR / Data Protection Act (2018) and will ensure we have the necessary staffing, resources, management structure and mechanisms in place so that Data Protection compliance is well-managed.

We will make every effort to ensure that we comply with the six principles of good practice for information handling and use.

If you are successfully shortlisted for interview and/or offered a job with Brandon Trust then the details around your application, offer and clearances (such as references, criminal records checks etc) will also be held on Brandon Trust networks and systems.

If you do not want us to use your personal data in this way, please do not register your details on our site.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

### Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

Our application process includes a question relating to your right to work in the UK. If you declare you do not have the right to work in the UK, the system will automatically not progress your application any further. Our system notifies you to confirm this and provides details of how you can contact us if you believe you have answered the question incorrectly.

You will not be subject to any other decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

## Cookies

Please click here to view iCIMS privacy policy which includes a section on their Cookie Policy (see section on Cookies and Similar Technologies)
https://www.icims.co.uk/legal/privacy-notice-website/

## Storage of your personal information

Brandon Trust requires everyone who has access to your information to treat the data as confidential and to seek to maintain its security. Your personal data will be used solely by Brandon Trust and will not be shared with third parties other than those previously mentioned for the recruitment process, except that your data may be disclosed to the third-party vendor that services the system and that requires access to the data within the system to provide its services. Brandon Trust requires this company to adequately safeguard your personal data and not use it for any unauthorised purposes. This applies also to the services provided by our Corporate IS Department.

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for (generally for up to one year), including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

If you become an employee, we will keep your information in the iCIMS system to make it easier for you to apply for other roles in Brandon. You have the right to have this data removed from this system.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. If you are unsuccessful in your application, we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

Upon your request, we will remove your personal information from our systems once we are no longer legally required to hold your data to defend against claims arising from the recruitment process.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

### How do we protect data?

We make sure that we have the right technical controls in place to protect your personal details. Our network is protected and routinely monitored. We ensure that your information is only accessible to appropriately trained staff, volunteers and contractors. Details of these measures are available upon request.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

We use some external companies to collect or process personal data on our behalf. We do comprehensive checks on these companies before we work with them. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

## Your rights

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your application process with us.

Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. To do this, please send us a letter telling us what information you want to see which includes proof of your identity to:

Head of IS
Brandon Trust
Olympus House
Patchway
Bristol
BS34 5TA

Under certain circumstances, by law you also have the right to:

- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- Request the transfer of your personal information to another party.

You can make the above requests by logging in to your iCIMS applicant dashboard and selecting the action you wish to take. If you have any problems please contact our recruitment team at recruitment.admin@brandontrust.org

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please log in to your iCIMS applicant dashboard and select the action you wish to take. If you have any problems please contact our recruitment team at recruitment.admin@brandontrust.org Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

You can contact our data protection officer via email at info@brandontrust.org or via our postal address. Please mark the email or envelope 'Data Protection Officer'.

If you believe that we have not complied with your data protection rights, you can complain to the Information Commissioner.

**What if you do not provide personal data?**

You are under no statutory or contractual obligation to provide data to us during the recruitment process. However, if you do not provide the information, we may not be able to process your application properly or at all.

You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.

## COVID-19 Data Protection Privacy Notice for staff, bank workers and job candidates

**Updated March 2021**

Brandon Trust may seek to collect, process and share your personal data in response to the COVID-19 pandemic, which is above and beyond what would ordinarily be collected, to ensure your safety and well-being and to protect the health and safety of the clinically vulnerable people we support.

Such information will be limited to what is proportionate and necessary, taking into account the latest guidance issued by the Government and health professionals, in order to manage and contain the virus. This may include information on COVID-19 testing and vaccinations.

Due to the nature of the COVID-19 pandemic, we may also need to process your information to ensure our public body funders are able to meet their legal obligations where such information is required in the public interest or for official purposes.

Steps will be taken to anonymise the data and general statistics/numbers used, wherever possible.

**Data security and retention**

- Data will be held securely, in line with our policies. We will only hold this data for as long as it allows us to meet the purposes above. The retention period will be confirmed as more information around the virus, testing, vaccines etc become available.
- We will only share data for the purposes above, and will do so via secure means, anonymising data wherever we are able to.
- Data will only be shared with those who need it be meet the purposes set out above.

**Basis for collecting this information**
The lawful bases under the GDPR for processing and sharing information are:

- Article 6(1)(f) processing is necessary for our legitimate interests or the legitimate interests of a third party.
- Article 9(2)(h) (the processing is necessary for health or social care purposes)

The legitimate interests that we have identified which require us to process your data are as follows:

- to ensure we can provide a safe working environment for our colleagues, and to protect the health and safety of the clinically vulnerable people we support.

- to enable us to provide information about the workforce to local authorities and other public bodies who may provide us with funding, to enable them to meet their legal obligations where such information is required in the public interest or for official purposes.

We have considered the balance between our reason for processing and your rights and freedoms as a data subject to ensure that the processing is justified.

## Changes to our privacy policy

We reserve the right to update this privacy notice at any time. Any changes we may make to our privacy policy in the future will be posted on this page (and, where appropriate, notified to you by e-mail). Your continued use of this site after changes have been posted constitutes your acceptance of this privacy and confidentiality policy as amended.

## Do you have any questions or feedback about this policy?

If you have any questions or feedback about this policy, please let us know by emailing recruitment.admin@brandontrust.org