Data Protection & Privacy Policy

Our Data Protection Officer at the time off issuing this policy is the Secretary. Any questions about this policy should be addressed to them. If they are no longer the Data Protection Officer, you can find out who is by contacting the Chair via our postal address is 1 Eastfield Road, Westbury-on-Trym, Bristol BS9 4AD.

1 Overview

1.1 We need to gather and use information or 'data' about you as part of our day to day activities and to manage our relationship with you. This policy sets out the things we must tell you about data protection.

1.2 We take the security and privacy of your data seriously and intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security.

1.3 This policy applies to current and former employees, workers, volunteers, apprentices and consultants. It also applies to applicants for financial assistance. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy.

1.4 We will only hold data for as long as necessary for the purposes for which we collected it.

1.5 The Organisation is a 'data controller' for the purposes of your personal data. This means that we decide how and why we process your personal data.

1.6 This policy explains how we will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Organisation.

2 Data Protection Principles

2.1 Personal data must be processed in accordance with the following '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up-to-date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are responsible for ensuring and demonstrating compliance with these principles.

3 How we define personal data

3.1 '**Personal data**' means information which relates to a person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper, or in/on other materials.

3.3 This personal data might be provided to us by you, or by someone else (such as a former employer, your doctor, or a credit reference agency or a referrer), or it could be created by us. It could be provided or created during the recruitment process, during the course of the employment contract, during the application process or during the course of the relationship. It could be created by the Secretary or other colleagues.

3.4 We will collect and use the following types of personal data about you:

- Recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments.
- Your contact details and date of birth.
- The contact details for your emergency contacts.
- Your gender.
- Your marital status and family details.
- Information about your employment contract (start & end dates, roles, hours, salary, pension, holiday entitlement and National Insurance Number)
- Your bank details and information in relation to your employment or financial support.
- Employees will also need to allow us to hold identification documents, disciplinary or grievance investigations, training records, IT systems)

4 How we define special categories of personal data

4.1 '**Special categories of personal data**' are types of personal data consisting of information about:

- your racial or ethnic origin;
- your political opinions;

- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health; and
- your sex life and sexual orientation.

We may hold and use any of these special categories of your personal data in accordance with the law. However, we do not outwardly seek to collect this type of data.

We may also hold and use personal data relating to criminal allegations, offences, proceedings and convictions.

5 How we define processing

5.1 'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storing;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6 How will we process your personal data?

6.1 We will process your personal data (including special categories of personal data) in line with our obligations under the 2018 Act.

6.2 We will use your personal data:

- for complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 12 below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to give us certain personal data, we may not be able to carry out some parts of the agreement between us. For example, if we do not have your bank account details, we may not be able to pay you.

7 Examples of when we might process your personal data

7.1 We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

7.2 We have to process your personal data to enable us to review our financial support and to decide how we can help you. Or tor any other reason which we may notify you of from time to time.

7.3 We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we ask for your consent to process a special category of personal data then we will explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the Secretary.

7.4 We will request and store information about you regarding criminal convictions from official bodies. This is necessary as you may be required to work alone with vulnerable adults during the course of your day to day work for the Organisation.

8 Sharing your personal data

8.1 Sometimes we might share your personal data with our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests, such as payroll or legal registrations.

8.2 We require those people and companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

8.3 We do not send your personal data outside the European Economic Area. If this changes, we will tell you. We'll also explain the protections that are in place to protect the security of your data.

9 How should you process personal data for the Organisation?

9.1 Everyone who works for, or on behalf of, the Organisation has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this and other relevant policies.

9.2 The Organisation's Data Protection Officer is responsible for reviewing this policy and updating the Trustees on the Organisation's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

9.3 Employees should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Organisation and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

9.4 Employees should not share personal data informally.

9.5 Employees should keep personal data secure and not share it with unauthorised people.

9.6 All email exchanges between the BBI Secretary, Trustees or outside parties and the Visitors should be conducted through the secure BBI email server

9.7 You should regularly review and update personal data. This includes telling us if your own contact or bank details change.

9.8 Employees do not save personal data to their own personal computers or other devices unless needed for the purposes of day to day work.

9.9 Personal data received as part of an application, financial update, amended banking or contact details should be transferred to the Secretary and once discussed at the Trustees meeting should be destroyed.

9.10 Agenda papers and minutes of meetings should be kept for one year and then destroyed.

9.11 Personal data for individuals who delay their application or receive one off support should be kept for one year and then destroyed. All other data is kept for the length of the relationship and then one further year for grant recipients and seven years for loan agreements.

9.12 Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer.

9.13 Employees must lock drawers and filing cabinets. And not leave paper that contains personal data lying about.

9.14 Employees should not leave laptops or paper files in vehicles or in public premises unattended.

9.15 Employees should not take personal data away from Organisation's premises without authorisation from the Secretary.

9.16 Personal data should be shredded and disposed of securely when finished with it.

9.17 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you under our Disciplinary Policy.

9.18 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our Disciplinary Policy and you could be dismissed.

10 How to deal with data breaches

10.1 If this policy is followed, we should not have any data breaches. But if a breach of personal data occurs (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours, where feasible.

10.2 If you are aware of a data breach you must contact the Data Protection Officer immediately and keep any evidence you have in relation to the breach.

11 Subject access requests

11.1 Data subjects can make a 'subject access request' ('SAR') to find out what information we hold about them. This request must be made in writing. If an employee receives a SAR they should forward it immediately to the Data Protection Officer who will coordinate a response.

11.2 To make a SAR in relation to your own personal data, you should write to the Data Protection Officer. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by up to two months.

11.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request. We normally work on the basis that any request which will take more than a day to deal with is likely to be manifestly excessive, and in those circumstances we believe a reasonable charge is 7 hours pay.

12 Your data subject rights

12.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

12.2 You have the right to access your own personal data by way of a SAR (see above).

12.3 You can correct any inaccuracies in your personal data by contacting the Data Protection Officer.

12.4 You have the right to request that we erase your personal data where we were not entitled under law to process it, or where it is no longer necessary to process the data for the purpose for which it was collected. You can request erasure by contacting the Data Protection Officer.

12.5 During the process of requesting that your personal data is corrected or erased, or while you are contesting the lawfulness of our processing, you can

ask for the data to be used in a restricted way only. To do this, contact the Data Protection Officer.

12.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

12.7 You have the right to object if we process your personal data for the purposes of direct marketing.

12.8 You have the right to receive a copy of your personal data and, with some exceptions, to transfer your personal data to another data controller (Trustee). We will not charge for this and will in most cases aim to do this within one month.

12.9 With some exceptions, you have the right not to be subjected to automated decision-making.

12.10 You have the right to be notified of a data security breach concerning your personal data where that breach is likely to result in a high risk of adversely affecting your rights and freedoms

12.11 In most situations we will not rely on your consent as a lawful ground to process your data. If we do request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Data Protection Officer.

12.12 You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has more information on your rights and our obligations.