DATA PROTECTION POLICY

BATH WELCOMES REFUGEES

REGISTRATION NUMBER: 1171442

ICO REGISTRATION NUMBER: ZA253093

Contents

1 Scope

Bath Welcomes Refugees, here after referred with the abbreviation BWR, charity registration number 1171442, with a registered address at The Island House, Midsomer Norton, Radstock, BA3 2DZ is committed to being fully compliant with all applicable UK and EU data protection legislation in respect of personal data, as well to safeguarding the rights and freedoms of persons whose information BWR may process pursuant to the UK General Data Protection Regulation 2020 (UK GDPR), the Data Protection Act 2018 (DPA) and any other applicable legislation. In this document all such legislation is collectively referred to as 'data protection legislation'.

This policy applies to all employees of BWR including contractors and subcontractors and to all volunteers, and any other persons that are authorised to access the data for which BWR is the controller.

This policy should be read in conjunction with the following BWR documents:

- Confidentiality policy
- Safeguarding policy
- SAR Policy
- Employment Handbook
- Volunteer Agreement

2 Definitions used in this policy

Data controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data processor: natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Protection Lead/accountable person: is the member of BWR's team who oversees data protection obligations and procedures.

Data subject: refers to any living person who is the subject of personal data (see above for the definition of 'personal data') held by BWR. A data subject must be identifiable by name, ID, address, online identifier or other factors such as physical, physiological, genetic, mental, economic or social.

Information Commissioner's Office (ICO)*:* the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Personal data: means any information that identifies, directly or indirectly, a data subject.

Processing: refers to any action taken in relation to personal data including, but not limited to, collection, adaptation, alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination or deletion, whether by automated means or otherwise

Special categories of data: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership biometric data (where used for identification purposes) data concerning health; data concerning a person's sex life or sexual orientation.

3 The appointment of a Data Protection Officer and a Data Protection Lead

BWR has assessed the need for a Data Protection Officer and has decided that this role is not required at this time. This decision is reviewed on an annual basis and its findings are recorded. The Data Protection Lead (accountable person) can be contacted via email: DPLead@bathwelcomesrefugees.org.uk .

4 The seven principles of data protection

BWR is committed to adhering to Article 5 of the UK GDPR which lists all the seven principles of data protection:

- **lawfulness, fairness and transparency:** BWR is committed to process data lawfully, fairly and in a transparent manner
- **purpose limitation**: BWR collects personal data for specified, explicit and legitimate purposes. BWR doesn't further process data in a manner that is incompatible with those purposes
- **data minimisation:** BWR is committed to process data that is adequate, relevant and limited to what is necessary
- **accuracy:** personal data are kept accurate and kept up to date
- **storage limitation:** BWR is committed to keep personal data for no longer than necessary
- **integrity and confidentiality**: BWR processes data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage
- **accountability**: BWR is able to demonstrate compliance

4.1 Lawfulness, fairness and transparency

4.1.1 Lawful basis

BWR identifies a lawful basis every time it starts processing personal data. Please see section 5 for more information on the six lawful bases of processing data.

4.1.2 Privacy notice

BWR is committed to informing all data subjects about the processing of their data beforehand so that they can make an informed decision about whether to provide that data. A service user privacy notice is made available to anyone who wants to know more about how we process data of the data subjects. Additionally, an HR privacy notice is made available to job applicants, freelancers, trustees and employees. We will provide an easy read version of the privacy notice to specific categories of data subjects, namely the refugees, asylum seekers and their families that BWR works with.

BWR has complied with Art 13 and 14 of the UK GDPR which list the content that needs to be included in the privacy notice and shorter statement.

BWR may periodically change how personal data is processed. BWR will inform the data subjects, accordingly, as required by the data protection legislation.

4.2 Purpose limitation

BWR collects personal data for specified, explicit and legitimate purposes and the data are not further processed in a manner that is incompatible with those purposes.

BWR may extend a purpose to cover new processing, as long as the new purpose is compatible with the old. Compatibility is measured according to the 'reasonable expectation' the data subject may have. BWR needs to process information to carry out its work, meet objectives and comply with the contractual obligations of funders. BWR will only ever collect information that is needed to carry out its work, improve its services, report to funders, contract holders and partners and to fulfil any request that data subjects make, personalise services to best meet data subjects' needs and to keep track of the impact and quality of our work.

The purpose of the data processing is included in the Privacy notice.

4.3 Data minimisation and accuracy

BWR is committed to the quality of the data that it collects and processes. This means that the data must be:

- adequate
- relevant
- limited to what's necessary
- accurate
- kept up to date

In order to guarantee data quality, volunteers receive clear guidance and training, and briefings during meetings in reference to personal data collection and processing.

BWR will periodically review of all methods of data collection, checking that they are still appropriate, relevant, and not excessive.

BWR is aware of the importance of collecting and maintaining accurate personal data. We will assume that information submitted by data subjects is accurate at the date of submission. Data subjects are promptly informed via the privacy notice (easy read leaflet available) that they are responsible for ensuring that the personal data held by BWR is accurate and up to date.

All staff and volunteers are required to update BWR as soon as reasonably possible of any changes to personal information, to ensure records are always up to date.

BWR shall, on an annual basis, carry out a review of all personal data controlled by BWR and decide whether any data are no longer required to be held for the stated purposes and where required, arrange for that data to be deleted or destroyed in accordance with the requirements of the Data Protection Legislation.

4.4 Storage limitation

BWR aims not to keep data subjects' data longer than is necessary. When we no longer need the data, we will dispose of the information securely and may use specialist external companies to do this.

In some cases, retention will be based on legal considerations. In other cases, the reason may be more practical or based on organisational decisions. Data subjects are informed about our retention periods through the privacy notice. Personal data is retained according to the retention period mentioned in the privacy notices, and is destroyed or deleted in a secure manner as soon as the retention date has passed.

Data that is kept for long periods of time is examined and amended, if necessary.

4.5 Integrity and Confidentiality

BWR maintains appropriate, technical and organisational security to protect personal data from unauthorized access or intrusion. This may include the friends and family members of staff.

BWR limits access to the data to those employees and volunteers who need such access in connection with providing services to data subjects, or for other legitimate purposes.

We will strive to train our employees and volunteers about our data protection practices.

All employees and volunteers are responsible for keeping secure any personal data controlled by BWR. Under no circumstances except safeguarding, may any personal data be disclosed to

any third party unless BWR has provided express authorisation or has entered into a confidentiality agreement, a data processor agreement, or a data sharing agreement with the third party (see section 8).

4.5.1 Bring your own devices policy

This section applies when volunteers of BWR use their personal devices to process data for which BWR is the controller.

It is important to ensure that personal devices and the information they contain are appropriately protected. This may require the use of a strong passcode to access the device. The passcode must not be shared with anyone. Software must be regularly updated.

When volunteers use personal emails and WhatsApp for communicating with service users any personal data should not be stored on their devices. When personal emails or WhatsApp or other messaging services are used to transfer service users' personal data onto BWR's own systems, the personal data must be deleted immediately once the transfer has taken place.

Other members of a household that use a device must not be able to access any business-related information. For example, an additional account passcode should be used to prevent unauthorised access (BWR's preference is for the device not to be accessible to other individuals).

The volunteer will regularly review the information on devices and delete copies from the device when no longer needed.

When a device is no longer required or is obsolete (for example because it is to be replaced) or when a volunteer leaves BWR, all information belonging to BWR must be securely deleted from any personal devices.

4.5.2 Confidentiality

BWR operates under a policy of confidentiality. BWR is committed to providing confidential services to their service users, and ensuring that all personal data are treated as confidential, and collected, processed and retained in line with data protection law.

In certain situations, information may need to be shared with third parties, and BWR will obtain the consent of its service users before sharing such information via its consent form. For safeguarding reasons, it may sometimes be necessary to share information without consent, in accordance with the guidelines set out in BWR's Safeguarding Policy.

4.6 Accountability - demonstrating Compliance

In accordance with legal requirements, BWR keeps records to demonstrate the steps taken to comply with the GDPR:

- **The Activity, Incident and Risk reporting spreadsheet** keeps a log of key information such as discussions and decisions about data protection, identified risks, any personal data breaches and response, training of staff and volunteers, requests to exercise any rights by data subjects and management of those requests, notifications to the ICO
- **Legitimate interests' assessments** (LIA) that have been carried out (see section 5.4 for more information)
- **Data protection impact assessments** (DPIA) that have been carried out to justify the approach where processing poses particular risks (such as processing of special category of data) – see section 7.3 for more information
- **Data protection policy** which includes most procedures relating to data protection
- **Privacy notice** for data subjects (see section 4.1.2)
- **Processors agreements** with database, CRM and cloud providers and other data processors (see section 8 for more information)
- **Data sharing agreements** (also called information sharing protocol) with other data controllers or joint controllers (see section 8 for more information)
- **Appropriate privacy document** which may be completed in some circumstances outlined by the DPA (2018) when processing special category of data or criminal records

5 The six lawful bases for processing personal data (including special category of data)

BWR processes personal data by identifying a 'lawful basis' chosen from the six possibilities set out in Article 6 of the UK GDPR:

- with consent of the data subject
- for a contract involving the data subject
- to meet a legal obligation
- to protect any personal vital interests
- for government and judicial functions
- in BWR's legitimate interests provided the data subject's interests are respected

The most common lawful bases that BWR identifies are legitimate interest, consent, contract and legal obligation.

When data processing poses particular risks (such as the processing of special category data - see section *7.3 Risk Assessment* for more details), BWR will complete a Data Protection Impact Assessment (DPIA) to justify the data protection approach.

When processing special categories of data or criminal records (see section 6) without the consent of the data subject, data protection law requires BWR to identify another lawful basis under Art 6 of the UK GDPR other than consent, supported by one of the exemptions of Art 9 (2) which might need to be furtherly supported by the DPA 2018. When processing criminal records, the lawful basis identified in Art 6 needs to be additionally supported by the DPA (2018).

BWR may complete an Appropriate Policy document for the processing of special categories of data and criminal data without consent of the data subjects as required by law.

5.1 Consent

If BWR chooses consent as its 'lawful basis', it means that the data subject has given their consent to the processing of their personal data for one or more specific purposes. BWR will gather a proof of that consent to demonstrate that the data subject has consented to processing of their personal data (as per Article 7.1 of the UK GDPR). The data subject still has the right to withdraw their consent at any time (as per Article 7.3 of the GDPR). Please see section 7.2 for more information on data subject's rights.

Consent to the processing of personal data by the data subject must be:

- Explicit - demonstrated by active communication between the data controller and the data subject and must not be inferred or implied by omission or a lack of response
- Freely given and should never be given under duress, when the data subject is in an unfit state of mind or provided on the basis of misleading or false information
- Specific and informed (it should cover the controller's name, the purposes of the processing and they types of processing activities)
- A clear and unambiguous indication of the wishes of the data subject
- In relation to sensitive data, consent may be provided in writing; if given verbally must be acknowledged in writing

BWR understands that Consent is for the time being and may review and refresh consent as appropriate.

Consent will not be the condition for processing data where a service or product is purchased.

5.1.1 Consent and minors

BWR may gather consent directly from minors if they are 16 or older.

If BWR supports a young person under 16, BWR may:

- gather consent from a parent or carer
- gather consent from a local authority that acquired parental responsibility when the minor is made subject to a care order by the court
- gather the young person's consent subsequently to an assessment of competence made and documented by a relevant staff member

A young person's consent may override consent gathered from their parents or carers.

5.2 Contract

BWR identifies contract as its lawful basis when processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract.

5.3 Legal obligation

BWR identifies legal obligation as a lawful basis when processing is necessary for compliance with a legal obligation to which the controller is subject.

5.4 Legitimate interest

BWR chooses legitimate interest as its lawful basis, a Legitimate Interest assessment may be completed to show what BWR's interest is and that it is legitimate, to show why the processing is necessary in pursuing this interest, to consider potential impact on any data subjects' rights and freedom and to measure whether the data subject might reasonably expect us to process their data. An opt-out option may be made available to the data subject. Data subjects always have a right to object to the processing of their data.

6 Data subjects and data specifications

BWR collects personal information from different groups of data subjects:

- Service users (refugees, asylum seekers and their families)
- volunteers
- job applicants
- web and social media data subjects
- attendees of events
- freelancers
- donors
- employees
- trustees

Our privacy notice will explain the different kinds of data we collect and the lawful basis for processing this. We process normal categories of data and we may also collect special category data and criminal data.

Criminal records are not formally special category data, however, under the Data Protection Act 2018, criminal records data receive the same additional protection as special category data.

For more information on how we process special categories of data and criminal records, please see section 5.5.

7 Additional compliance obligations

BWR is committed to complying with the additional obligations in reference to the UK GDPR and the Data Protection Act 2018. These include:

- breach notification
- data subject's rights
- risk assessment
- by design and by default
- protection of children
- fees

7.1 Breach notification procedures

Article 4.12 of the UK GDPR defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, authorisation, and authorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

These are the steps taken by BWR in case of a data breach:

- Any staff member or volunteer who discovers a personal data breach is required to immediately inform their line manager or team leader and the data protection lead.
- The staff member/volunteer and the line manager /team leader need to ensure that the breach is not still occurring and take any immediate mitigating action that may reduce the impact of the breach.
- In accordance with Article 33.1 of the GDPR, BWR must report the data breach to the ICO within 72 hours 'unless the personal data breach is unlikely to result in a risk to the rights and freedom of natural persons.' The decision to report such a breach will be made by BWR. If the breach is reported, the accountable person will make the report using the ICO's website. Factors that may determine whether a breach is reportable include:
    - sensitivity of the categories of data. For example, data identifying a health condition.
    - quantity of data concerned.

- whether there is a potential for a high risk of harm to the data subjects concerned

Mitigating factors that may be considered when not reporting a breach:

- The data are retrievable.
- Evidence that data breach has been contained and that those who may have access will not process the data in such a way as to cause harm or distress to the data subjects concerned.

- If the data breach is reported to the ICO, BWR will make available any documents or records that the ICO requires to peruse the inquires. BWR will cooperate with the ICO with any request and record any guidance the ICO gives in accordance with the breach in the activity incident and risk reporting spreadsheet (please see section 4.6 for more information on this spreadsheet).
- If the data breach is likely to result in a high risk to the rights and freedoms of natural persons (e.g., where the breach could result in ID theft or fraud; physical harm; significant humiliation and/or damage to reputation) BWR would need to communicate the breach of their personal data without undue delay to the affected individuals. In some circumstances, BWR may decide to not inform the individuals if by doing so it would cause more damage and anxiety to the data subjects than the data breach itself.
- If the individuals are informed of the data breach, BWR will also ask if they want to log a formal complaint to the ICO for how their personal data has been managed.
- The data breach is then logged into the activity incident and risk reporting spreadsheet in order to identify lessons BWR can learn and the changes that can be made. If the data breach is reported to the ICO, the case number supplied by the ICO will be recorded in the activity incident and risk reporting spreadsheet.
- Train staff where required to ensure the breach doesn't happen again.

The agreements that BWR stipulates with data processers include a clause requiring them to inform BWR immediately or in any event within 24 hours of them becoming aware of a breach. This is to allow BWR to make a report to the ICO within the 72 hours.

If a data subject has been harmed by a breach of data protection legislation, they can take the controller to court for compensation.

Contractors, subcontractors, and other parties may be subject to appropriate legal action in accordance with BWR's processor agreement. If there is a possibility that the breach could amount to a criminal offence, the matter shall be referred immediately to the relevant authorities.

7.2 Data subjects' rights

BWR is fully aware of the data subject rights described in Articles 15 to 22 of the UK GDPR and these are listed in the privacy notice. The data subjects' rights include:

1. The right to be informed

2. The right of access
3. the right of rectification
4. the right to be forgotten (erasure)
5. the right to restrict processing
6. the right to data portability
7. the right to object processing
8. rights in relation to automated decision making and profiling

Additional rights of the data subjects:

- the right not to receive direct marketing
- the right to claim damages should they suffer any loss as a result of a breach of the provisions of the GDPR
- the right to complain - right to request that the ICO carry out an assessment

If data subjects wish to exercise any rights, they can contact BWR by email at DPLead@bathwelcomesrefugees.org.uk or via other contact information displayed on our website. They are reminded of their rights and how to exercise them in the privacy notice they receive (see section 4.1.2)

All staff members are trained to recognise an incoming request to exercise any right, to understand when the right applies and to pass it on without delay to the designated person.

All requests from data subjects to exercise any rights are recorded into the Activity, Incident and Risk reporting spreadsheet (please see section 4.6 for more information on this spreadsheet).

Under certain circumstances, mostly described in Schedules 2-4 of the DPA (2018), BWR may not need to comply with the request by a data subject to exercise one of their rights. Those circumstances will be assessed on a case-by-case basis.

7.2.1 The right to be informed

Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. BWR is committed to complying with this right and we do so via the privacy notice (see section 4.1.2).

7.2.2 The right of access and SAR procedure

A data subject has the right to make access requests in respect of personal data that is held and disclosed. To understand how we deal with Subject Access Requests, please view our SAR policy.

7.2.3 The right of rectification

BWR is aware of the provisions in Article 16 of the UK GDPR: if the data subject becomes aware that BWR is holding incorrect information about them, they have the right for it to be corrected, and if their information is incomplete, they can also submit additional information to be added.

In conjunction with Article 19 of the GDPR, BWR will inform anyone to whom data has been disclosed of the right exercised by the data subject, unless this 'proves impossible or involves disproportionate effort'. BWR will also inform the data subject which recipients data has been disclosed, if they ask.

7.2.4 The right to be forgotten (erasure)

If a data subject asks BWR to delete their information, as stated in Article 17, BWR will do so without undue delay when:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws consent (if that is the basis on which the processing is taking place), and where there is no other legal ground for the processing;
c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation;
f) the personal data have been collected in relation to the offer of online services to a child.

In addition, if BWR has made the information public, it must try to get it erased in other locations as well. In conjunction with Article 19 of the UK GDPR, BWR will inform anyone to whom data has been disclosed, unless this 'proves impossible or involves disproportionate effort'. BWR will also inform the data subject which recipients data has been disclosed to, if they ask.

There are exceptions to the 'right to be forgotten' for reasons relating to freedom of expression, public health, archiving, research and statistics, legal claims and legal obligation.

There may also be circumstances where BWR has no choice but to retain data, for example, historical safeguarding issues or to mark a record for suppression in order to ensure that no direct marketing is sent to that individual in the future. BWR will process a request for erasure without undue delay and within one month of receipt. BWR gives particular weight to any request for erasure if the request relates to data collected from children.

7.2.5 The right to restrict processing

The data subject shall have the right to obtain from BWR restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling BWR to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- BWR no longer needs the personal data for the purposes of the processing, but the data is required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pursuant to Article 21(1) pending verification of whether the legitimate grounds of BWR override those of the data subject.

7.2.6 The right to data portability

This right applies when processing is based on consent or a contract between BWR and the data subject and the process and the processing is taking place 'by automated means'. It allows data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

Data subjects are entitled to receive from BWR a copy of any personal data they have provided, in a 'structure, commonly used and machine-readable format', so that they can provide the data to a different controller.

7.2.7 The right to object to processing

Data subjects can object to any processing of their data that BWR is carrying out on the lawful basis of legitimate interests. BWR will stop processing if not able to demonstrate 'compelling legitimate grounds'.

7.2.8 Rights in relation to automated decision making and profiling

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. Profiling refers to any form of personal data processing that is automated, with the intention of assessing personal aspects of a data subject or analysing a data subject's employment performance, economic status, whereabouts, health, personal preferences and behaviour.

The data subject has the right to object to profiling and a right to be informed of the fact that profiling is taking place, as well as the intended outcome(s) of the profiling. The data subject has the right not to have decisions made about them solely by automated processing if this has a significant effect on them, unless the decision is necessary in conjunction with a contract between the data subject in the controller or the data subject has provided an explicit consent.

BWR does not currently undertake automated decision making.

7.2.9 The right not to receive direct marketing

Every data subject has the right not to receive direct marketing if that is their choice.

7.2.10 The right to claim damages in case of data breach

If a data subject has been harmed by a breach of data protection legislation, they can take the controller to court for compensation. See section 7.1 for more information about data breach.

7.2.11 The right to complain

If data subjects wish to make a complaint or share a concern, they should be firstly encouraged to liaise directly with BWR. They can make a complaint or send an email to complaints@bathwelcomesrefugees.org.uk or to the email address for the Data Protection Lead (DPLead@bathwelcomesrefugees.org.uk). BWR will respond within 5 working days and take steps for the resolution of the complaint within 28 days.

As stated in the privacy notice, BWR will inform data subjects that they can also make a complaint to the ICO and request that the ICO carries out an assessment of whether any of the provisions of the UK GDPR have been breached. Data subjects can remain anonymous if they wish.

7.3 Risk Assessment

Risk Assessment is an important part of the accountability of an organisation. It is vital that BWR is aware of all risks associated with personal data processing and it is via its risk assessment process that BWR is able to assess the level of risk.

It is BWR's policy not to transfer or share data into an environment that is not considered compliant with UK or EU data protection law.

Where personal data processing is carried out by using new technologies, or when a high risk is identified in relation to the rights and freedoms of natural persons, BWR is required to engage in a risk assessment of the potential impact, also known as a 'Data Protection Impact Assessment' (DPIA). More than one risk may be addressed in a single DPIA. BWR has agreed upon a procedure for completing a DPIA and this is set out in its Legitimate Impact Assessment. This procedure is always followed where there is a need to measure risk. The procedure is completed by the Data Protection Lead and if necessary, the opinion of a professional Data Protection Practitioner is taken into account.

In addition to this, and if the outcome of a DPIA points to a higher risk than BWR intended and personal data processing could result in distress and/or may cause 'damage' to the data subjects, it is for the Data Protection Lead to decide whether BWR ought to proceed, and the matter should be escalated. In turn, the Data Protection Lead may escalate the matter to the regulatory authority (prior to commencing the new project) if significant concerns have been identified.

7.4 By design and by default

This policy includes procedures in relation to data protection across BWR, involving different staff members, teams and delivery. As BWR aims towards full compliance and therefore also towards data protection "by design and by default", we will aim to embed these procedures into our operating guidelines as appropriate and proportionate to our resources and capacities.

The goal of this principle would mean that in BWR, everyone who starts a new project or sets up a system or a process would aim to incorporate data protection as a matter of course, consulting the Data Protection Lead. Consideration of the data protection implications should be a standard check point before any project or system is signed off.

7.5 Protection of children

The UK GDPR does not treat children particularly differently from adults, but BWR is committed to take appropriate precautions, in particular:

- When we are considering 'legitimate interests' as our lawful basis, we will be particularly careful not to override the interests of the data subject
- When providing information to children about how their data will be processed, we will ensure that they will genuinely be able to understand it
- Requests to exercise data subject's rights will have a particular weight when involving data around children

For more information on minors and consent, please see section 5.1.1.

7.6 Registration to the ICO and fees

BWR has registered with the Information Commissioner as a data controller that engages in the processing of personal information identifying data subjects directly or indirectly.

BWR pays an annual fee to ICO, as required by law for data controllers.

8 Data sharing - working with other organisations

As any other organisation, BWR may collaborate with:

- data processors
- joint controllers
- separate controllers

All third parties we work with who have or may have access to personal data of our data subjects, will either comply with this policy, or we will ensure that their data protection policy aligns with this policy.

8.1 Data Processors

A data processor is a company or organisation, or an individual who is not an employees or volunteers, that processes data on behalf of the data controller (BWR in this policy).

Before deciding to use a particular service, BWR would check the terms and conditions and decide whether it is compliant before deciding to use that service.

With freelancers, external researchers and IT companies, BWR stipulates a Processor Agreement or a contract including data protection provisions, as outlined by Article 28.3 of the UK GDPR.

BWR remains responsible for what happens to the data and remains liable for any mistakes of the data processors. In the contract with the data processor, BWR may include a provision that requires the data processor to reimburse BWR.

8.2 Joint Controllers

Art 26 of the UK GDPR, define *joint controllers* as two or more data controllers which jointly determine the purpose and means of processing. When BWR collaborates with a data controller, the parties must agree to a Joint Controller Agreement which could include the following:

- who it applies to
- general data protection principles, including the basic principle of confidentiality
- the purposes for which information will be shared
- the lawful basis on which sharing will take place
- how each partner will discharge their transparency obligations, and whether all parties will use the same form of words to ensure consistency
- procedures for sharing information, and in particular for obtaining and recording consent from the data subject (if this is the lawful basis)
- procedures to ensure that all parties have the same understanding of how to comply with the data protection principles regarding data quality and retention
- access and security procedures
- procedures for ensuring that the handling of data subjects' rights is consistent and fully compliant
- procedures for raising concerns or resolving difficulties
- how the agreement will be managed and kept under review

The purpose for which information will be shared, the lawful basis on which the sharing will take place and general information about each data controller will need to be included in the privacy notice for those data subjects affected by the data sharing and the collaboration between BWR and the joint controller.

8.3 Separate Controller

BWR may collaborate with another organisation which is a separate controller as information are merely disclosed to one other. In this case, BWR may agree to a Data Sharing Agreement with the other separate controller(s), which defines the following:

- parties involved in the agreement
- purpose for which information will be shared
- the lawful basis on which the sharing will take place
- other organisations involved in the data sharing
- what data items will be shared (including special category of data)
- procedures to comply with data subjects' rights
- governance arrangements

The purpose for which information will be shared, the lawful basis on which the sharing will take place and general information about each data controller will need to be included in the Privacy notice for those data subjects affected by the data sharing and the collaboration between BWR and the other separate controller(s).

9 International Data Transfer

Where personal data are stored outside of the UK and the EU, safeguards to protect personal data may include but are not limited to the UK Addendum used in conjunction with the EU Standard Contractual Clauses (SCCs), or UK International Data Transfer Agreement (IDTAs). Such safeguards will be subject to Transfer Risk Assessments (TRAs).

10 Changes to this policy

This Policy is updated regularly by the Data Protection Lead when required. It is reviewed annually by the Data Protection Lead and the board of trustees.