Data Protection Policy

1. Policy Statement

1.1 This policy sets out how PBE processes the personal data of data subjects, including the personal data of job applicants and the personal data of all staff, volunteers, contractors, consultants, clients, customers, suppliers and other third parties.

1.2 PBE will obtain, store, access and disclose certain personal data about living individuals when carrying out its activities. PBE recognises the importance of the correct and lawful treatment of personal data; not handling information in a proper and secure manner can lead to real harm and distress to the person that the information relates to, and cause harm to PBE's reputation.

1.2 This policy applies to all personal data that we process, regardless of the media on which those personal data are stored, e.g. electronically, on paper or on other materials.

1.3 Personal data is information about identifiable living individuals. It includes their names, email addresses, telephone numbers, credit and debit card numbers and HR records. Information may be personal data even if the individual will only be identifiable when the information is tied to other data held by PBE or other data that it is likely PBE will hold. Each individual to whom the information relates to is known as a "data subject".

1.4 PBE is committed to being clear and transparent about how we collect and use personal data and to complying with our data protection obligations. Protecting the confidentiality, security and integrity of the personal data that we process is also of paramount importance to our business operations.

1.5 PBE will process personal data relating to you in accordance with this policy, the data protection legislation and the Staff Privacy Notice which has been issued to you.

1.6 This policy applies to all members of staff. It is non-contractual and does not form part of any employment contract, worker agreement, consultancy agreement or any other contract for services.

1.7 As a member of staff, you are yourself a data subject and you may also process personal data on the PBE's behalf about other data subjects. The data protection legislation contains important principles affecting personal data relating to data subjects. The purpose of this policy is to set out what we expect from you and to ensure that you understand and comply with the rules governing the processing of personal data to which you may have access in the course of your work, so as to ensure that neither PBE nor you breach the data protection legislation.

1.8 Any breach of this policy or any breach of the data protection legislation will be regarded as misconduct and will be dealt with under the Disciplinary Policy. A significant or deliberate breach of this policy, constitutes a gross misconduct offence and could lead to your summary dismissal. If you are not an employee, you may have your contract with PBE terminated with immediate effect.

1.9 PBE's Data Protection Officer (DPO) has responsibility for data protection compliance within the business. You should contact them if you have any questions about the operation of this policy or you need further information about the data protection legislation, or if you have any concerns that this policy is not being or has not been followed.

1.10 If you wish to make an internal complaint that this policy is not being or has not been followed, you can also raise this as a formal grievance under PBE's Grievance Policy.

2. The Data Protection Principles

2.1 Under the data protection legislation, there are six data protection principles that PBE and all members of staff must comply with at all times in their personal data processing activities. In brief, the principles say that personal data must be:

i. Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).

ii. Collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).

iii. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

iv. Accurate and, where necessary, kept up to date; every reasonable step must also be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy).

v. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed (storage limitation).

vi. Processed 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, using appropriate technical or organisational measures (integrity and confidentiality).

PBE is responsible for, and must be able to demonstrate compliance with, these data protection principles. This is called the principle of accountability.

2.2 This means PBE will:

- Consider each reasonable request of an individual to access his or her personal information, under a "data subject access request"; and
- Where appropriate, provide individuals with the opportunity to express preferences relating to receiving marketing material and will honour those preferences.
- Ensure all personal data is kept secure
- Seek to ensure that it has measures in place to prevent unauthorised or unlawful processing of personal information and against accidental loss, destruction or damage.
- Not transfer data to third parties or to countries outside the EEA without adequate protection.

3. Subject Access

3.1 All individuals who are the subject of personal data held by PBE are entitled to be:

- Told whether any personal data is being processed;
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- Given a copy of the personal data (subject to such redaction as PBE considers necessary to comply with its data protection obligations and/or to protect its commercial interests); and
- Given details of the source of the data (where this is available).

3.2 If personal details are inaccurate, they can be amended upon request.

3.3 PBE aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 30 days of a written request.

3.4 Subject to certain conditions, and in certain circumstances, data subjects have the right to:

- Be informed – this is normally satisfied by issuing them with an appropriate privacy notice
- Request rectification of their personal data - this enables them to have any inaccurate or incomplete personal data we hold about them corrected or completed, including by their providing a supplementary statement

- Request the erasure of their personal data - this enables them to ask us to delete or remove their personal data where there's no compelling reason for their continued processing, e.g. it's no longer necessary in relation to the purpose for which they were originally collected or if there are no overriding legitimate grounds for the processing
- Restrict the processing of their personal data - this enables them to ask us to suspend the processing of their personal data, e.g. if they contest the accuracy and so want us to verify the accuracy or the processing is unlawful but they don't want the personal data to be erased
- Object to the processing of their personal data - this enables them to ask us to stop processing their personal data where we are relying on the legitimate interests of the business as our lawful basis for processing and there is something relating to their particular situation which makes them decide to object to processing on this ground
- Data portability - this gives them the right to request the transfer of their personal data to another party so that they can reuse them across different services for their own purposes
- Not be subject to automated decision-making, including profiling - this gives them the right not to be subject to a decision based solely on the automated processing of their personal data, if such decision produces legal effects concerning them or similarly significantly affects them
- Prevent direct marketing - this enables them to prevent our use of their personal data for direct marketing purposes
- Be notified of a data breach which is likely to result in a high risk to their rights and freedoms

3.5 If a data subject invokes any of the rights above, you must take steps to verify their identity, log the date on which the request was received and seek advice from our DPO.

4. Staff Responsibilities

4.1 All staff are responsible for:

- Checking that any personal data that they provide to PBE is accurate and up to date
- Informing PBE of any changes to information which they have provided, e.g. changes of address
- Checking any information that PBE may send out from time to time, giving details of information that is being kept and processed
- Complying with this policy and the data protection principles at all times in your personal data processing activities where you are acting on behalf of PBE in the proper performance of your job duties and responsibilities

4.2 You must also comply with the following guidelines at all times:

- Only access personal data that you have authority to access and only for authorised purposes
- Only allow other members of staff to access personal data if they have the appropriate authorisation and never share personal data informally
- Do not disclose personal data to anyone except the data subject unless the data subject has given their explicit consent to this
- Strictly follow PBE's requirements in relation to passwords to be used before releasing personal data
- Only transmit personal data between locations by e-mail if a secure network is in place, e.g. encryption is used for e-mail
- Ensure any personal data you hold are kept securely, either in a locked non-portable filing cabinet or drawer if in hard copy, or password protected or encrypted if in electronic format, and comply with PBE rules on computer access and secure file storage
- Do not access another member of staff's personal data, e.g. their personnel records, without authority
- Do not obtain or disclose personal data (or procure their disclosure to a third party) without authority or without PBE's consent

- Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which it would be inappropriate to share with that data subject
- Do not remove personal data, or devices containing personal data, from the workplace with the intention of processing them elsewhere unless this is necessary to enable you to properly carry out your job duties and responsibilities, you have adopted appropriate security measures (such as password protection, encryption or pseudonymisation) to secure the data and the device and it has been authorised by your line manager
- Ensure that, when working on personal data when away from your workplace and with the authorisation of your line manager, you continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security
- Do not store personal data on local computer drives, your own personal computer or on other personal devices
- Do not make unnecessary copies of personal data and keep and dispose of any copies securely, e.g. by shredding hard copies
- Remembering that compliance with the data protection legislation and the terms of this policy is your personal responsibility

5. Publication of Charity Information

Information published as a part of journalistic material is exempt from data protection laws. This includes, for example, information about staff contained within externally circulated publications. Any individual who wishes for information concerning themselves to be excluded from PBE publications should immediately inform the person whom they report to.

6. Subject Consent

The need to process data for normal purposes has been communicated to all data subjects. In some cases, if the data is sensitive, for example information about health, religious belief, racial or ethnic origin, trade union membership, political opinions, mental health, sexual life or criminal offences explicit, specific consent to process the data must be obtained. Processing may be necessary to operate Charity policies, such as health and safety and equal opportunities.

7. Retention of Data

7.1 PBE will keep some forms of information for longer than others. All staff are responsible for ensuring that information is not kept for longer than necessary and is destroyed or erased when no longer required.

7.2 When personal data are no longer needed for specified purposes, you must ensure that they are destroyed, erased or anonymised in accordance with PBE's rules on data retention.

7.3 Details of the Data Retention Periods are available in the Appendix.

8. Intellectual Property

8.1 All staff are required to promptly disclose to PBE any idea, invention or work which is relevant to (or capable of use in) the business of PBE now or in the future made by you in the course of your performance of your duties, whether alone or with any other person.

8.2 All staff acknowledge that all Intellectual Property Rights (as defined below) subsisting (or which may in the future subsist) in any such ideas, inventions or works or which in any other way arise from their performance of your duties, whether alone or with any other person will, on creation, vest in and be the exclusive property of PBE.

8.3 For the purposes of this clause "Intellectual Property Rights" means any and all patents, trademarks, service marks, rights in designs, get-up, trade, business or domain names, goodwill associated with the foregoing, copyright (including rights in computer software and databases), topography rights (in each case whether

registered or not and any applications to register or rights to apply for the registration of any of the foregoing), rights in inventions, knowhow, trade secrets and other confidential information, rights in databases and all other intellectual property rights or forms of protection of a similar nature or having equivalent or similar effect to any of these which may now or in the future subsist anywhere in the world for the full period thereof and all extensions or removals thereof.

9. Changes to this policy

9.1 PBE will review this policy at regular intervals and reserves the right to update or amend it at any time and from time to time.

9.2 It is intended that this policy is fully compliant with the data protection legislation. However, if any conflict arises between the data protection legislation and this policy, PBE will comply with the data protection legislation.

Definitions

In this policy, the following words and phrases have the following meanings:

"Consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them.

"Criminal records personal data" means personal data relating to criminal convictions and offences and personal data relating to criminal allegations and proceedings.

"Data protection legislation" means the EU General Data Protection Regulation (GDPR), the Data Protection Act 2018 and any other applicable primary or secondary legislation as may be in force in the UK from time to time.

"Data subject" means a living identified or identifiable individual about whom the Company holds personal data.

"Member of staff" is any director, employee, worker, agency worker, apprentice, intern, volunteer, contractor and consultant employed or engaged by the Company.

"Personal data" is any information relating to a data subject who can be identified (directly or indirectly) either from those data alone or by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that data subject. It excludes anonymised data, i.e. where all identifying particulars have been removed.

"Processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, disseminating, restricting, erasing or destroying. It also includes transmitting or transferring personal data to third parties.

"Special categories of personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data, data concerning the physical or mental health of a data subject or data concerning a data subject's sex life or sexual orientation.

Appendix - Data Retention Guidance and Schedule

Data Retention Guidance

1. Principles

PBE complies with the data protection principles and will ensure that:

- Staff records are regularly reviewed to ensure that they remain adequate, relevant and limited to what is necessary.
- Staff records are kept secure and are protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- When records are destroyed, whether held as paper records or in electronic format, PBE will ensure that they are safely and permanently erased.

2. Recruitment Records

2.1 PBE retains personal information following recruitment exercises to demonstrate, if required, that candidates have not been unlawfully discriminated against and that recruitment exercises are conducted in a fair, consistent and transparent way.

2.2 The Applicants Privacy Notice advises applicants how long PBE expects to keep their personal information for, once a recruitment decision has been made. This is likely to be for six months from the communication of the outcome of the recruitment exercise which takes account of the time limit to bring a tribunal claim.

2.3 Information relating to successful applicants will be transferred to their employment record. This will be limited to that information necessary for the working relationship and, where applicable, that required by law.

3. Staff Records

PBE will retain personal data in line with the recommended retention periods for particular employment records set out in legislation, referred to in the table below. However, it also has regard to legal risk and may keep records for up to seven years (and in some instances longer) after employment or work with the company has ended.

4. Data Retention Schedule

Type of employment record	**Retention period**
Recruitment records These may include: Completed online application forms or CVs. Equal opportunities monitoring forms. Assessment exercises or tests. Notes from interviews and short-listing exercises. Pre-employment verification of details provided by the successful applicant. For example, checking qualifications and taking up references. (These may be transferred to a successful applicant's employment file.) DBS checks. (These may be transferred to a successful applicant's employment file if they are relevant to the ongoing relationship.)	Six months after notifying applicants of the outcome of the recruitment exercise.
Right to Work Checks	Three years after the termination of employment.
Contracts	
These may include: Written particulars of employment. Contracts of employment or other contracts. Documented changes to terms and conditions.	While employment continues and for seven years after the contract ends.
Payroll, salary and sickness records	
Payroll, salary and sickness records Details on overtime. Bonuses. Expenses/Benefits Redundancy payments/calculations	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made
PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Payroll and wage records	These must be kept for six years from the financial year-end in which payments were made. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.

Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for seven years after the working relationship ends.
Travel and subsistence.	While employment continues and for seven years after employment ends.
Record of advances for season tickets and loans to employees	While employment continues and for seven years after employment ends.
Personnel records	
These include: Qualifications/references. Consents for the processing of special categories of personal data. Annual leave records. Performance Review Records. Disciplinary procedures. Grievance procedures. Death benefit nomination and revocation forms. Resignation, termination and retirement.	While employment continues and for seven years after employment ends.
Records in connection with working time	
Working time opt-out	Three years from the date on which they were entered into.
Records to show compliance, including: Time sheets for opted-out workers. Health assessment records for night workers.	Three years after the relevant period.
Maternity and Family Leave records	
Family Leave payments/dates on unpaid leave Dates of family leave. Maternity certificates/ Adoption certificates	Four years after the end of the tax year in which the family leave pay period ends.
Accident records	
These are created regarding any reportable accident, death or injury in connection with work.	For at least four years from the date the report was made.