



YOUNG BRISTOL DATA PROTECTION POLICY

Last Reviewed: April 2021

Next Review Due: April 2024

Our thanks to Burges Salmon for their help and guidance in producing this Policy



CONTENTS

Clause	Heading	Page
1	ABOUT THIS POLICY	1
2	DEFINITION OF DATA PROTECTION TERMS	1
3	DATA PROTECTION PRINCIPLES.....	2
4	FAIR AND LAWFUL PROCESSING	3
5	PURPOSES OF PROCESSING	3
6	ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING	4
7	ACCURATE DATA.....	4
8	TIMELY PROCESSING	4
9	PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS.....	4
10	DATA SECURITY	5
11	TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA.....	6
12	DISCLOSURE AND SHARING OF PERSONAL INFORMATION	6
13	DEALING WITH SUBJECT ACCESS REQUESTS	7
14	CHANGES TO THIS POLICY	7

1 ABOUT THIS POLICY

- 1.1 Everyone has rights with regard to how their Personal Data is handled. During the course of our activities we will collect, store and process Personal Data about our customers, suppliers, employees contractors, trustees, volunteers and the young people we work with, and we recognise the need to treat it in an appropriate and lawful manner.
- 1.2 Data Users are obliged to comply with this policy when Processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action.
- 1.3 The types of Personal Data that we may be required to handle include details of current, past and prospective employees, suppliers, customers, young people, and others that we communicate with. The Personal Data is subject to certain legal safeguards specified in the Data Protection Act 1998 ("**the Act**") and other regulations.
- 1.4 This policy sets out the rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transferring and destruction of Personal Data. It sets out the basis for our Processing of Personal Data that we collect from Data Subjects, or that is provided to us by Data Subjects or other sources.
- 1.5 This policy does not form part of any employee's contract of employment and may be amended at any time.
- 1.6 The Data Protection Compliance Manager is responsible for ensuring compliance with the Act and with this policy. That post is held by Lee Williams, Chief Executive Officer, LW@youngbristol.com. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Compliance Manager.

2 DEFINITION OF DATA PROTECTION TERMS

- 2.1 **Data** is information which is stored in certain paper-based filing systems or electronically on a computer or other media.
- 2.2 **Data Subjects** for the purpose of this policy include all living individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data.
- 2.3 **Personal Data** means data relating to a living individual who can be identified from that Data (or from that Data and other information in our possession). Personal Data can be

factual (such as, a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

- 2.4 **Data Controllers** are the people who, or organisations which, determine the purposes for which, and the manner in which, any Personal Data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the Data Controller of all Personal Data used in our business.
- 2.5 **Data Users** include employees whose work involves using Personal Data. Data Users have a duty to protect the data they handle in accordance with our data protection policy at all times.
- 2.6 **Data Processors** include any person or organisation that is not a Data User that processes Personal Data on our behalf and on our instructions. Employees of Data Controllers are excluded from this definition but it could include suppliers which handle Personal Data on our behalf.
- 2.7 **Processing** is any activity that involves use of the Data. It includes obtaining, recording or holding the Data, or carrying out any operation or set of operations on the Data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.
- 2.8 **Sensitive Personal Data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive Personal Data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

3 DATA PROTECTION PRINCIPLES

- 3.1 Anyone Processing Personal Data must comply with the eight enforceable principles of good practice. These provide that Personal Data must be:
 - (a) processed fairly and lawfully;
 - (b) processed for limited purposes and in an appropriate way;
 - (c) adequate, relevant and not excessive for the purpose;
 - (d) accurate;
 - (e) not kept longer than necessary for the purpose;
 - (f) processed in line with the Data Subjects' rights;

- (g) secure;
- (h) not transferred to people or organisations situated in countries withoutadequate protection.

4 FAIR AND LAWFUL PROCESSING

- 4.1 The Act is not intended to prevent the Processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject.
- 4.2 For Personal Data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the Data Subject has consented to the processing, or that the processing is necessary for the performance of a contract with the Data Subject, for the compliance with a legal obligation to which the Data Controller is subject or for the legitimate interest of the Data Controller or the party to whom the Data is disclosed. When Sensitive Personal Data is being processed, additional conditions must be met. When Processing Personal Data as Data Controllers in the course of our business, we will ensure that those requirements are met.

5 PURPOSES OF PROCESSING

- 5.1 Personal Data may only be processed for legal, personnel, administrative and management purposes or for any other purposes specifically permitted by the Act. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the Data Subject must be informed of the new purpose before any processing occurs.
- 5.2 The likely purposes for which employees' Personal Data may be Processed by us include, without limitation:
 - recruitment, promotion, training, redeployment and/or career development,such as references, CVs and appraisal documents;
 - administration and payment of wages, such as emergency contact details and bank/building society details;
 - calculation of certain benefits including pensions;
 - disciplinary or grievance issues;
 - performance management purposes and performance review;
 - recording of communication with employees and their representatives;
 - compliance with legislation;

- provision of references to financial institutions, to facilitate entry onto educational courses and/or assist future potential employers; and
- staffing levels and career planning.

5.3 We will process Sensitive Personal Data primarily where it is necessary to enable us to meet our legal obligations, in particular to ensure adherence to health and safety laws, and for equal opportunities monitoring purposes. In most cases, we will not process Sensitive Personal Data without your consent.

6 ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

6.1 We will only collect Personal Data to the extent that it is required for the specific purpose notified to the Data Subject.

7 ACCURATE DATA

7.1 Personal Data we hold should be accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date Data.

7.2 To ensure the Data we hold is accurate and up to date, you must notify us as soon as possible of any change in your personal details (e.g. change of name, address, telephone number, loss of driving licence where relevant, next of kin details etc).

8 TIMELY PROCESSING

8.1 We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all Data which is no longer required.

9 PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

9.1 We will process all Personal Data in line with Data Subjects' rights. Data Subjects have a right to:

- (a) request access to any Data held about them by a Data Controller;
- (b) prevent the processing of their Data for direct-marketing purposes;
- (c) ask to have inaccurate Data amended;
- (d) prevent Processing that is likely to cause damage or distress to themselves or anyone else.

10 DATA SECURITY

- 10.1 We will take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.
- 10.2 We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a third party Data Processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.
- 10.3 We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:
- (a) **Confidentiality** means that only people who are authorised to use the Data can access it.
 - (b) **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed.
 - (c) **Availability** means that authorised users should be able to access the Data if they need it for authorised purposes. Personal Data should therefore be stored on our central computer system instead of individual PCs.
- 10.4 Security procedures include:
- (a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
 - (b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
 - (c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.
 - (d) **Equipment.** Data Users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- 10.5 Data Users must comply with our security measures and report any concerns regarding the loss of Personal Data to their line manager immediately. Failure to do so may result in disciplinary action under our Disciplinary Procedure, up to and including dismissal without notice.

11 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

11.1 We may transfer any Personal Data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- (a) the country to which the Personal Data are transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- (b) the Data Subject has given his consent;
- (c) the transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the Data Subject, or to protect the vital interests of the Data Subject;
- (d) the transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims;
- (e) the transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the Data Subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

11.2 Subject to the requirements in clause 10.1 above, Personal Data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff may be engaged in, among other things, the fulfilment of contracts with the Data Subject, the processing of payment details and the provision of support services.

12 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

12.1 We may disclose Personal Data we hold to third parties:

- (a) In the event that we sell or buy any business or assets, in which case we may disclose Personal Data we hold to the prospective seller or buyer of such business or assets;
- (b) If we or substantially all of our assets are acquired by a third party, in which case Personal Data we hold will be one of the transferred assets;
- (c) If we are under a duty to disclose or share a Data Subject's Personal Data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subject or other agreements;
- (d) If it is necessary to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other

companies and organisations for the purposes of fraud protection and credit risk reduction.

- 12.2 We may also share Personal Data we hold with selected third parties for the purposes set out at 5.2.

13 DEALING WITH SUBJECT ACCESS REQUESTS

- 13.1 A formal request from a Data Subject for information that we hold about them must be made in writing and accompanied by a £10 administration fee. Any employee who receives a written request should forward it to their line manager immediately.

- 13.2 When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if the following conditions are met:

- (a) we will check the caller's identity to make sure that information is only given to a person who is entitled to it; and
- (b) we will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

- 13.3 Employees should refer any request to their line manager for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

14 CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where appropriate, we will notify Data Subjects of those changes by mail or e-mail.

Signed:



Ben Hardy Chair of Trustees

Signed:



Lee Williams Chief Executive

Date: April 2021