Ref:	[unique]
Version	
Review	[Date]

LIVE BORDERS

DATA PROTECTION POLICY

Version Control

Version	Author	Change description	Consultation	Board approval
2	Sheila brodie	Updated to reflect Governance & Project officer role and changes to SAR, put into new template		
3	Sheila Brodie	Updated to reflect DPA 2018	N/A	

Contents [right click and update field, select entire table]

1. Purpose

1.1 This Policy exists to inform staff of their responsibilities and their rights in relation to Data Protection. It offers guidance in relation to data security and information sharing. It outlines the Data Protection Principles.

1.2 The data protection policy ('the policy') will apply to all personal data/information held and/or processed by the Company and all employees and Members of Live Borders ('the Company') and any partner organisation (voluntary or otherwise), contractor, or agent performing work on behalf of or in conjunction with the Company.

1.3 Compliance with the policy and associated procedures are a condition of employment or any other method of delivering a service or function on behalf of or with the Company. Violations of the policy may subject an employee or other data holder / controller to appropriate disciplinary action, in accordance with the Company's current disciplinary procedures.

1.4 It is the Company's policy to fully comply with the Data Protection Act 2018 and all other related statutory, criminal and civil obligations to which the Company is required to adhere including the GDPR. This applies to the retrieval, storage, processing, retention, destruction and disposal of 'personal data'.

2. Definitions

2.1 The Act uses the term 'personal data'. For information personal data means any recorded information held by us and from which a living individual can be identified. It will include a variety of information including names, addresses, telephone numbers, photographs of people and other personal details. It will include any expression of opinion about a living individual or any indication of our intentions about that individual. The Data Protection Act applies to personal information processed by any forms of medium, including CCTV images, photographs, and digital images. Any processing of such data must be in accordance with the principles of the Data Protection Act and this policy.

3. Scope

3.1 This policy applies to all staff and contractors (freelancers) working for Live Borders and to the Board of Trustees. The Company will ensure that they hold and process personal information only to support those activities we are legally entitled to carry out.

3.2 Personal data relating to employees may be collected by the Company for the purposes of:

i. recruitment, promotion, training, redeployment and / or career development, such as references, CVs and appraisal documents

ii. administration and payment of wages, such as emergency contact details and bank/building society details

iii. calculation of certain benefits including pensions

iv. disciplinary or grievance issues

v. performance management purposes and performance review

vi. recording of communication with employees and their representatives

vii. compliance with legislation

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

4. Key Principles -Data Protection Principles

4.1 We will comply with the eight enforceable data protection principles by making sure that personal data is:

1. fairly and lawfully processed

2. processed for limited purposes

3. adequate, relevant and not excessive

4. accurate and kept up to date

5. not kept longer than necessary

6. processed in accordance with the individual's rights

7. secure

8. not transferred to countries outside the European Economic area unless the country to which the data is to be transferred has adequate protection for the individuals

4.2 Training

4.2.1 All staff will be trained in the basics of data protection as soon as practical after their start date as part of the induction process.

4.2.2 Staff who work on computer systems that hold or process personal information, or who use the information associated with those systems, will be trained by the systems administrator or line manager.

4.3 Information security

4.3.1 Printouts, CDs and Memory sticks and other devices containing personal information that need to go from one office to another should be delivered to a specific person or secure area, and not left lying about for collection

4.3.2 You must supervise external maintenance and support staff to ensure personal data is protected.

4.3.3 Ensure personal data is destroyed appropriately when no longer required, including data on computer hard drives/memory sticks etc.

4.3.4 When dealing with personal information on portable equipment, whether or not it belongs to us, you must make sure no unauthorised person can get access to or see any personal data, either held on computer or paper files.

4.5 Subject Access

4.5.1 The Data Protection Act gives you the right to access the personal data held about you by the Company.

4.5.2 The Company will endeavour to process all written subject access requests within the statutory one month deadline. Where the Company is unable to process the request within the timeframe, the data subject should be notified as soon as possible of any potential delay, the reasons for such a delay, and the date when their information will be made available.

4.5.3 Subject access requests should be made by emailing foi@liveborders.org.uk or in writing or in person to the Data Protection Officer, Live Borders, Melrose Road, Galashiels, TD1 2DU. Applications for subject access will not be accepted by telephone.

4.6 Direct Marketing

4.6.1 The Company will not participate in direct marketing practices where individuals do not consent to the use of their personal information for this purpose.

4.6.2 All individuals must be given the opportunity to opt-in to receive material at the point of data collection, or opt-out of receiving material at the point of distribution.

4.6.3 The appropriate opt-in and opt-out mechanisms must be put in place where third party marketing or advertising materials are distributed to named individuals. In situations where this cannot be feasibly done, the materials must not be distributed.

4.7 Third Parties

4.7.1 Any person working in a partnership capacity (voluntary or otherwise), working as a contractor (or agent) - whether directly or indirectly in the employ of the Company - should sign a confidentiality (non-disclosure) agreement before being granted access to personal information.

4.7.2 The Data Protection Officer must be consulted prior to entering into any contracts. Contracts for processing of information by a third party on behalf of the Company will require the insertion of confidentiality clauses and specific advice must be sought from Legal advisor. The Company must be satisfied that the Information Security measures adopted by the third party are adequate before access to information is granted.

4.8 Data Sharing

4.8.1 Appropriate information sharing protocols must be in place before personal information will be processed on our behalf by third parties. These protocols will be reviewed, amended and updated on a regular basis. Guidance should be sought from the Governance and Projects Officer.

4.8.2 Individuals will be informed, at the point of data capture, of:

i. The identity of the data controller

ii. The identity of any organisation other than the Company with whom the information may be shared

iii. The purpose or purposes for which the data are or are intended to be processed

4.8.3 Live Borders website provides publically accessible information about the companies approach to customer and supplier data sharing and security. www.liveborders.org.uk

4.8.4 Individuals have the right to access information the Company holds on them and that a reasonable fee may be charged if the Subject Access Request is manifestly unfounded, or excessive. All forms which gather personal data will have an Fair Processing notice at the bottom of each form.

4.9 Complaints

4.9.1 Any complaints received regarding the Data Protection policy or its associated procedures, including subject access requests, should be handled through the Company Complaints system in the first instance.

5 Responsibilities

5.1 CEO

All aspects of compliance with the Act, and associated legislation, within the Company.

5.2 Managers

Responsible for themselves as employees and for ensuring that all staff are aware of and adhere to this policy.

5.3 Employees

5.3.1 Adhering to this policy

5.3.2 Recording information (in compliance with the Data Protection Notification) about an individual which is relevant, and should be aware that they may be required to justify what has been written and be prepared for that information to be released as part of a subject access request.

5.3.3 Ensure they are familiar with the requirements of the Data Protection Act 2018 and the GDPR.

5.3.4 Disclose personal information to employees on a 'need to know' basis only dependent upon the nature or role of their employment, or in order to carry out ad hoc tasks and duties. The need for access must be clearly demonstrated at all times.

5.3.5 All employees must follow good practice as indicated by the Data Protection Act and any such codes of practice issued by the Office of the Information Commissioner or the Company, when processing personal data.

5.3.6 Inform the Data Protection Officer of any new requirement, system, product or process that requires data to be held.

5.3.7 Consult the Data Protection Officer and ensure appropriate documentation is in place prior to any data sharing arrangement is entered into.

5.3.8 Reporting suspected breaches of the data protection policy to their own management or to the Data Protection Officer.

5.3.9 Deal with any subject access requests as per this policy

5.3.10 Ensuring the Company's files are accurate and up to date, and so that the Company is able to contact you or, in the case of an emergency, another designated person, you must notify the Company 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).

5.4 Other

The Governance & Projects Manager is the designated Data Protection Officer for the Company and is responsible for:

i. Developing, publishing, maintaining and administering the data protection policy

ii. Maintaining our Notification Entry with the Information Commissioner

iii. Providing an annual return on the use and processing of personal information within the Company, and for making any amendments to the register entry as and when they occur

iv. Assisting other employees in understanding the significance of Data protection and GDPR.

Trustees of the Company are responsible for:

v. Members of the Board are entitled to have access to data which is necessary for him/her to carry out any official duties as is the case with employees. The requirement for access must be clearly demonstrated.

vi. Reporting suspected breaches of the data protection policy to their own management or to the Data Protection Officer.

6 Compliance

6.1 Any employee who is found to have inappropriately divulged personal information will be subject to investigation under the Company's disciplinary procedure, which may result in dismissal and possible legal action.

7 Consultation

7.1 The Directors, HR Manager, Finance and Performance Manager have been consulted and their comments noted.

8 Related Policies, Forms and Information

8.1 Related Policies

8.1.1 Live Borders Disciplinary Policy

8.2 Related Information

8.2.1 The Data Protection Act 2018
8.2.2 The General Data Protection Regulations
8.2.3 Privacy Regulations 2003
8.2.3 Data Protection Guidance
8.2.4 GDPR staff guide

8.3 Related Forms

8.3.1 Live Borders Non-Disclosure Agreement

9 Monitoring and review

9.1 This policy has been Equality Impact Assessed

9.2 The Governance & Projects Officer is responsible for monitoring the effectiveness of this policy and will review the implementation of it on a regular basis, assessing its adequacy, suitability and effectiveness.