Data Protection Policy

1. Introduction

What does this document do? This is an internal data protection policy which sets out the standards which the Charity has adopted in its handling of personal data (including data relating to employees, volunteers, customers, suppliers, donors, corporate partners and other third parties). It documents how the Charity seeks to ensure that it complies with the Data Protection Laws (as defined in section 2.2 below) and tells all staff what is expected of them where their role involves handling personal data.

1.1 Like all organisations, in order to operate Bookmark Reading Charity (referred to in this policy as "we", "us", "our" or the "Charity") needs to handle large quantities of information. Where that information relates to individuals, then it is important to ensure that we comply with Data Protection Laws. This document sets out the standards that we have adopted in relation to the way that we handle personal data and explains to each individual who works in our organisation what is expected of them to the extent that their role involves handling personal data in some way. Organisations that fail to comply with data protection laws can potentially be fined up to EUR 20 million or 4% of worldwide turnover (whatever figure is higher).

1.2 It is important that everyone who works in our organisation (including trustees, employees, temporary workers, agency workers, contractors, interns, apprentices and volunteers) understands and operates to the standards set out in this policy when handling personal data. In this policy, we refer to those people as "Data Users".

1.3 The importance of this policy means that failure to comply with any requirement may lead to disciplinary action (employees), which may result in summary dismissal, or action in accordance with the Volunteer Problem Solving Policy (volunteers).

1.4 If you have any questions about this policy then please contact the Data Protection Officer, Dionne Campbell, Dionne.Campbell@BookmarkReading.org . We may amend this policy at any time. It does not form part of any employee's contract of employment.

1.5 This policy should be read alongside other policies which relate to how we use personal data, including the Data Retention and Destruction Policy, Data Breach Response Policy, IT and Data Security Policy, Subject Access Request Policy, Website Privacy Policy, Cookies Policy, Privacy Notice for Employees and Contractors and the Volunteer Privacy Policy.

1.6 Throughout this policy "staff" includes trustees, employees, temporary workers, agency workers, interns, apprentices and volunteers.

2. What is personal data?

2.1 Personal data is any information relating to an identified or identifiable natural person ('data subject'), an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. . The personal data that we handle in the Charity may have come from a number of sources. and is likely to include a person's name, address, staff number or location. Some personal data is provided to us directly from individuals (for example, by completing forms or by corresponding with us by mail, email, phone or otherwise). We also receive personal data about individuals from other sources (including, for example, business partners, payment and delivery services, credit reference agencies and others).

2.2 The data protection laws within the UK consist of the General Data Protection Regulation 2016/679 (as it forms part of domestic law in the UK by virtue of Clause 3 of the European Union (Withdrawal) Act 2018) ('UK GDPR'), the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426). set out clear rules on what we can and cannot do with personal data. In this policy, we refer to those laws collectively as the "Data Protection Laws". Data Laws apply whenever the Charity "processes" personal data. "Processing" is a broad term, which means any activity carried out in relation to personal data, including using, storing, transferring, or destroying personal data.

3. Your responsibilities

3.1 In summary, all Data Users should:

3.1.1 familiarise themselves with this policy and comply with its terms when processing personal data on our behalf;

3.1.2 familiarise themselves with our Website Privacy Policy, Volunteer Privacy Policy, and Privacy Notice for Employees and Contractors (together our "Privacy Notices") which set out how we use personal data;

3.1.3 inform the Data Protection Officer before initiating any new data processing activities which are not covered by our Privacy Notices;

3.1.4 forward any requests or complaints received from any individuals in respect of their personal data or the Information Commissioner's Office (the UK's data protection regulator) immediately to the Data Protection Officer so that they can be dealt with within any mandatory legal timescales; and

3.1.5 comply with our Data Breach Response Policy and notify any data breach immediately to the Data Protection Officer.

4. General principles

4.1 Data Users must observe the following principles when processing personal data:

4.1.1 only use personal data in a way that makes it clear to individuals what is being done with their personal data, and is fair, reasonable and compliant with Data Protection Laws;

4.1.2 use it in line with how we told the individual we would use it (via the Privacy Notice that we provide) and not for any other purposes;

4.1.3 personal data must be adequate, relevant and limited to what told the individual we would use it for.
4.1.4 data must be accurate and kept up to date;
4.1.5 data must not be kept for longer than we need it; and
4.1.6 data must be kept secure.

4.2 In addition, we must not send personal data to companies and people outside the UK and the EEA without following certain procedures. No personal data should be transferred outside of the UK and EEA. If you believe this to be required, please reach out to the DPO.

4.3 It is important that the Charity complies with these principles and that we are able to demonstrate that we have done so (this is known as the "accountability" principle). Therefore, it is important that you make a record of any personal data that you process and how the processing complies with those principles.

5. Fair and lawful processing

5.1 We must only process personal data if one or more of the lawful bases set out in the Data Protection Laws apply.

5.2 This means that we will only process personal data if:

5.2.1 the individual has given us their consent (we must ensure that the consent wording and mechanism for obtaining consent meet the requirements of the Data Protection Laws);
5.2.2 we need to process the personal data in order to perform a contract with the individual, or because they have asked us to take certain steps before entering into a contract;
5.2.3 the processing is necessary to comply with the law (not including contractual obligations);
5.2.4 the processing is necessary to protect someone's life;
5.2.5 the processing is necessary to perform a task in the public interest or for our official functions; or
5.2.6 the processing is necessary for the Charity's legitimate interest or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those interests.

5.3 Generally, Data Users should consult the Data Protection Officer who can confirm which is the most appropriate basis to rely on. We should always record our reasoning for choosing a particular lawful basis, so we can explain ourselves if an individual complains or the data protection regulator (ICO) asks us.

6. Sensitive personal data and criminal checks

6.1 Some of the information we hold as a Charity is particularly sensitive, (also known as "Special Category Data"), and we must be aware that special rules apply when we process Special Category Data.

6.2 This includes information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data (where it uniquely identifies them), or about their health, sex life or sexual orientation (special categories of personal data).

6.3 We will generally not collect and use such data unless the individual has given us explicit consent (for example, confirmed in writing that they agree to us holding their special categories of personal data) or we need it in order to fulfil our obligations as an employer or deployer in the case of volunteers. We will not disclose special categories of personal data to anyone outside of the Bookmark organisation without the consent of the individual See clause 7 (Obtaining consent) below for more information on how to get consent.

6.4 If you have any questions or concerns in relation to the processing of special category personal data, please contact our Data Protection Officer.

7. Obtaining consent

7.1 Sometimes we will need consent to use someone's personal data, for example if we are sending them marketing emails, or disclosing special categories of personal data to a third party. Where we need consent, we will ensure our consent wording and mechanisms for obtaining and recording consents comply with the Data Protection Laws.

7.2 Where we rely on consent for processing special categories of personal data, we will ensure that it is explicit (expressly confirmed in words rather than by any other positive action).

7.3 Whenever we request consent for processing, we will:

- 7.3.1 present the request for consent in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language;
- 7.3.2 not use pre-ticked opt-in boxes;
- 7.3.3 not make services conditional on consent to the processing of personal data that is not necessary for the performance of that contract (for example, marketing);
- 7.3.4 keep records of consent obtained so we can provide evidence if required; and
- 7.3.5 enable individuals to withdraw their consent at any time. Data Users should consult with the Data Protection Officer if they receive a request from an individual that wishes to withdraw his or her consent.

7.4 We must be mindful when relying on consent to process children's personal data, particularly where providing online services to children under the age of 13, that we may need to obtain parental or guardian consent. Data Users should consult the Data Protection Officer in relation to any processing of children's personal data to ensure that relevant compliance steps are addressed. More information on processing children's personal data can be found here: **Children and the UK GDPR | ICO.**

8. Processing for limited purposes

8.1 Personal data may only be processed for the specific purposes notified to the individual when the data was first collected or for any other purpose that is specified in the Charity's Privacy Notice or otherwise specifically permitted by Data Protection Laws.

8.2 This means, broadly, 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, we will inform the individual of the new purpose before any processing occurs, this can be done via the provision of the Charity's Privacy Notice.

9. Notifying individuals (privacy notices)

9.1 In order to satisfy the transparency requirements under the Data Protection Laws, when collecting personal data directly from individuals, we will ensure that they receive appropriate information about how we will use their data by giving them with our Privacy Notice.

9.2 The privacy notice must set out the following:

- 9.2.1 our name, the contact details of the Data Protection;
- 9.2.2 why we are processing individual's personal data and the lawful basis that applies (for example, consent or legitimate interests) when processing such personal data;
- 9.2.3 if we are processing the personal data on the basis of our or a third party's legitimate interests, we must explain what those interests are;
- 9.2.4 anyone with whom we will share the personal data (either their name or a general description of them) – this includes any customers or suppliers to whom we may pass the data;
- 9.2.5 details of transfers of the data outside the UK and EEA and safeguards we have put in place (for example, standard contractual clauses and the UK addendum);
- 9.2.6 how long we plan to retain the personal data, or the criteria used to determine the retention period in context of our Data Retention and Destruction Policy;
- 9.2.7 their rights (see clause 0 (
- 9.2.8 Individual rights) below);
- 9.2.9 if they have given us consent, that they have the right to withdraw the consent at any time;
- 9.2.10 their right to lodge a complaint with the ICO ;
- 9.2.11 whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the data; and
- 9.2.12 the existence of any automated decision-making which could have a legal or similar significant effect for the individual, and information about how decisions are made, the significance and the consequences.

9.3 If we receive personal data about an individual indirectly (for example, via third parties), we will provide the individual with the information in clause 8.2 above, as well as details of the categories of personal data we are processing and where we got it from (for example, whether it came from a public source), as soon as possible.

9.4 If we later need to use that personal data for a different or new purpose, we will tell the individual beforehand.

9.5 We have standard Privacy Notices in relation to personal data which set out the information above. If you are starting a new processing activity which is not covered by our Privacy Notices, please contact the Data Protection Officer.

10. Accurate data

We will ensure that personal data we hold is 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 and out-of-date data.

11. Minimal processing and data retention

11.1 We will not collect excess personal data or retain personal data for longer than we need it. This means:

11.1.1 we will only collect personal data to the extent that it is required for the specific purpose notified to the individual in our Privacy Notice provided to them;

11.1.2 we will not keep personal data longer than is necessary for the purpose for which it was collected; and

11.1.3 we will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required, in line with our Data Retention and Destruction Policy.

11.2 We will implement appropriate technical and organisational measures for ensuring that our systems allow us to do this.

11.3 We will also ensure that personal data is not automatically made accessible to an indefinite number of people and that access is appropriately limited. Staff will be assigned specific role profiles in our Salesforce platform to limit what data is accessible depending on their job role.

12. Direct marketing

12.1 We will only ever send business-to-consumer (B2C direct marketing to individuals who we have received explicit opt-in consent from . We request this consent from all volunteers at the point of registration. When we are sending business-to-business (B2B) direct marketing (e.g. to corporate subscribers), we will follow the 'legitimate interests' principle and send on the basis of 'implied consent'.

12.2 Data Users involved with direct marketing should be aware that particular rules apply when sending marketing to contacts, including post marketing and electronic marketing (for example, by SMS, email and where we call to sell services) and that we are required to comply with these rules.

12.3 Please contact the Data Protection Officer and the Head of Marketing and Communications for advice on direct marketing before starting any new direct marketing activity.

12.4 Individuals have the right to ask us to stop sending them marketing at any time. We will abide by any such request and notify the Data Protection Officer whenever an individual opts out of receiving marketing, so they can update the CRM system and notify the relevant teams and/or departments accordingly.

13. Individual rights

13.1 We will observe and process all personal data in line with individuals' rights under the Data Protection Laws, in particular the individual's rights to:

13.1.1 request access to any personal data held about them and other supplementary information (see *Requests from Individuals* below);
13.1.2 have inaccurate or incomplete personal data corrected;
13.1.3 object to us profiling them, sending targeted marketing to them;
13.1.4 withdraw their consent at any time;
13.1.5 have their personal data erased from our systems;
13.1.6 'block' or suppress our use of their personal data;
13.1.7 not to be subject to automated decisions (i.e. decisions made solely on a computer without human intervention) that produce legal effects or similarly significantly affect them, unless they have consented, or another exception applies; and
13.1.8 receive their data in a portable form.

13.2 Data Users should forward any requests or complaints received from individuals in respect of their personal data immediately to the Data Protection Officer so that they can be dealt with within any mandatory legal timescales. These rights are subject to some limitations and therefore it's important that the Data Protection Officer is notified as soon as possible.

14. Data protection procedures

14.1 As part of the accountability principle, we are required to:

14.1.1 keep records of processing we carry out;
14.1.2 integrate privacy measures and security controls into our processing activities ('data protection by design and default');
14.1.3 carry out a data protection impact assessment if our use of personal data is likely to result in high risk to the rights and freedoms of individuals (for example, where carrying out large-scale systematic monitoring, such as by CCTV or using a new technology); and
14.1.4 ensure our systems have appropriate functionality to allow us to fulfil any requests made by individuals (for example, for access to their data).

14.2 The Data Protection Officer should be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are followed.

15. Data security

15.1 We will ensure that appropriate measures are taken to keep data secure. Individuals may apply to the courts for compensation if they have suffered damage due to a breach of security and we may incur large fines if we are in breach of the Data Protection Laws. You may also be liable personally for fines or imprisonment if you steal or recklessly misuse personal data.

15.2 The Data Protection Laws require us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

15.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

15.3.1 **Confidentiality** means that only people who are authorised to use the data can access it.

15.3.2 **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

15.3.3 **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 (including SharePoint and Salesforce) instead of individual PCs.

15.4 Security procedures include:

15.4.1 **Entry controls.** Any unfamiliar person seen in entry-controlled areas should be reported.

15.4.2 **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind (personal data is always considered confidential).

15.4.3 **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed or wiped when they are no longer required.

15.4.4 **Equipment.** Data Users must ensure that individual monitors do not show confidential information to passers-by and that they lock or log off from their PC when it is left unattended.

15.5 Generally, to keep personal data secure you must not disclose personal data - in writing or verbally - to anyone not authorised to receive it, whether internal or external, and whether within or outside the workplace.

15.6 In addition to this policy, Data Users must comply with our IT and Data Security Policy, which sets out further information about how we keep personal data and other information secure.

16. Data breaches

16.1 We have specific obligations to report any breach of security involving personal data to the data protection regulator, the ICO. A 'personal data breach' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, theft, corruption or unauthorised disclosure of, or access to, personal data. This is more than just about losing information and includes any security incident (accidental or deliberate) which affects the confidentiality, integrity or availability of information – for example loss of a laptop or paper file or sending an email to the wrong recipient.

16.2 Data Users should notify the Data Protection Officer immediately of any breaches of security which lead or could lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data – for example loss of a laptop or paper file, or sending an email to the wrong recipient. This will allow us to:

16.2.1 investigate the failure and take remedial steps if necessary; and

16.2.2 make any applicable notifications within the mandatory legal timescales.

Please see our Data Breach Response Policy for more information on how to report data breaches.

17. Third parties

17.1 We will only use processors (for example, sub-contractors) who:

17.1.1 can assure us they meet the standards (including security standards) required by the Data Protection Laws; and

17.1.2 agree to comply with our procedures and policies or agree to put in place adequate measures themselves.

17.2 A written contract must be put in place with certain mandatory clauses prescribed by the Data Protection Laws. In the event that a third-party service provider is engaged who will process personal data on behalf of the Charity, additional data protection provisions must be included into any contract, and it is likely that further considerations may need to be addressed. Standard data processing l clauses can be obtained from the Data Protection Officer.

17.3 Additionally, we must take reasonable steps to monitor the third party service provider's performance of the relevant security and processing obligations.

18. Sharing of personal data

18.1 We may from time to time be asked to share personal data we hold:

18.1.1 with external providers, such as payroll, pension, insurance and occupational health providers;

18.1.2 with a third party in the event that we, our operations, or substantially all of our assets are acquired by such third party (in which case personal data will be one of the transferred assets);

18.1.3 in order to comply with legal obligations, or in order to enforce or apply a contract with an individual or other agreements; or to protect our rights, property, or safety of our staff, customers, volunteers, beneficiaries or others. This includes exchanging information with other companies and organisations for the purposes of safeguarding, fraud protection and credit risk reduction; or

18.1.4 With any third party that assists us in our ordinary course of business, including but not limited to third parties providing security checks, translation services, confidential shredding, impact reporting services, and other charitable services.

18.2 We will only share such information if we have a lawful basis and ensure we comply with any other relevant policies.

18.3 Where Data Users receive requests to share information, they should contact the Data Protection Officer for assistance. Where appropriate, the relevant companies should enter into a data sharing agreement setting out their respective rights and obligations.

18.4 We may share personal data with processors in accordance with the terms of this policy (see clause 17 (Third parties) above).

18.5 If data will be transferred outside the UK and EEA, see clause 19 (Sending personal data overseas) below.

19. Sending personal data overseas

19.1 We may be asked to transfer personal data to third parties which are located overseas or international organisations or to use sub-contractors based overseas.

19.2 The Data Protection Laws impose restrictions on the transfer of personal data outside the UK and EEA, to third countries or international organisations located in third countries. A third country is a country that is located outside of the UK and EEA which has not been deemed to provide an adequate level of protection to personal data in accordance with the Data Protection Laws.

19.3 Where we need to send an individual's personal data we hold outside the UK and EEA to a third country or make it accessible to people in a third country , we will need to follow certain procedures with regards to the contractual provisions that we implement and the assessments that we undertake.

19.4 Data Users should not transfer personal data to any third countries without first consulting the Data Protection Officer, who can ensure that the correct procedures have been followed and are in place.

20. Dealing with requests from individuals

20.1 Individuals may make a request for information we hold about them or other requests (for example, for portable data) orally or in writing.

20.2 We have to respond to certain requests from individuals in relation to their personal data within strict timescales, so it is very important that Data Users who receive a request should forward it to the Data Protection Officer immediately.

20.3 If the request is made by telephone, Data Users should take steps to verify the caller's identity and take a written record of the request. Data Users should not be bullied into disclosing information and should inform the Data Protection Officer of all such requests immediately.