Data Protection Policy

Aim of this Policy

The aim of this policy is to set out Doorstep Library's commitment to protecting personal data, to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This policy also highlights key data protection procedures within the organisation.

Who is covered by this Policy?

This policy applies to all employees, consultants, volunteers, service users, donors, partners and trustees and any other individual where personal information/data is collected

Introduction to Data Protection

Data Protection is the fair and proper use of information about people.

The Data Protection Act (DPA) 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and sits alongside the General Data Protection Regulation 2016/679 (GDPR). Under the DPA Doorstep Library falls under the general processing regime.

Doorstep Library will collect, store and process personal information on its employees, consultants, volunteers, service users, donors, partners and trustees to carry out its day-to-day operations, to meet its objectives and to comply with legal obligations.

What is Personal Data?

Personal Data is information about a particular living individual. For the purposes of Doorstep Library this includes employees, consultants, volunteers, service users, donors, partners and trustees.

What is Processing?

Almost anything you do with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing and deleting it.

What is a Controller?

A Controller is the person that decides how and why to collect and use the data. The Controller must make sure that the processing of data complies with data protection law. The name of the Controller within our organisation as specified in our notification to the Information Commissioner is Katie Bareham.

Under the Data Protection Guardianship Code, overall responsibility for personal data in a not-for-profit organisation rests with the governing body. In the case of Doorstep Library this is the Board of Trustees.

The governing body delegates tasks to the controller. The Controller is responsible for: understanding and communicating obligations under the Act/ Regulation;
identifying potential problem areas or risks; producing clear and effective procedures;
notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes.

All employed staff, consultants, trustees and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy may result in:
Employed staff and consultants – disciplinary proceedings;
Trustees and volunteers – termination of trusteeship or volunteering agreement.

What is GDPR?

The GDPR came into effect on 25 May 2018 and sets out the key principles, rights and obligations for most processing of personal data.
In line with the GDPR seven key principles Doorstep Library will ensure that personal data will:

- Be obtained lawfully, fairly and in a transparent manner
- Be obtained for a specific, explicit and legitimate purpose
- Be adequate, relevant and limited to what is necessary
- Be accurate and, where necessary, kept up to date;
- Not be held longer than necessary;
- Be processed in a manner that ensures appropriate security of the personal data
- The final principle is accountability. This highlights that the data controllers are responsible for complying with the principles

Key Principles of Personal Data Guardianship

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. Doorstep Library will seek to abide by this code in relation to all the personal data it processes, i.e.

- Accountability: those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.

- Visibility: Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- Consent: The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- Access: Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- Stewardship: Those collecting personal data have a duty of care to protect this data throughout the data life span.

Type of Information Processed

Doorstep Library processes the following personal information:

- Information on applicants for posts, including references;
- Employee information – contact details, bank account number, payroll information, supervision, appraisal and disciplinary notes;
- Volunteers – contact details, application form, interview notes, DBS reference number and expiry date, supervision notes, records of attendance and interactions;
- Supporters – contact details, interactions, donations made;
- Funders – contact details, amount granted/ donated;
- Users – information including, but not limited to, contact details, participation notes, ages of children, ethnic origin, schools attended, safeguarding concerns (notes), referral forms, feedback questionnaires and quotes.

Personal information is kept in the following forms:

- Paper based
- Electronic copy – on secure cloud servers/ database/Mailchimp

Groups of people within the organisation who will process personal information are:

- Employees
- Consultants
- Trustees
- Volunteers

Notification

The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis, as the law requires.

If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

Policy Implementation

To meet our responsibilities employees, consultants, volunteers and trustees will:

- Ensure any personal data is collected in a fair and lawful way;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised.

We will ensure that:

- Everyone managing and handling personal information is trained to do so;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures;
- Queries about handling personal information will be dealt with swiftly and politely.

Training

Training and awareness raising about the GDPR and how it is followed in this charity will take the following forms:

On induction, employees, consultants and trustees will receive copies of the:

- Data Protection Policy;
- Confidentiality Policy;

Staff will sign the Data Protection Declaration form to confirm understanding and adherence.

On induction volunteers will receive a copy of the Confidentiality Policy

Volunteers will sign the Volunteers' Commitment Form to confirm understanding and adherence to the Confidentiality Policy

General training/ awareness raising:

- Employees, consultants, trustees and volunteers will be informed of any material changes to the Data Protection Policy as and when they occur;
- Volunteers will be reminded of the principles of the Confidentiality Policy as part of their refresher training (ad hoc).

Gathering and Checking Information

Before personal information is collected, we will consider:
What information it is necessary to collect and for what purpose – employee, volunteer, supporter, user.

We will take the following measures to ensure that personal information kept is accurate:

- For users, volunteers will check personal details (such as age child) on an annual basis, through face-to-face questions during a regular session;
- Employees are responsible for ensuring that their personal information on Bright HR is kept up to date
- Consultants should notify the Head of Operations of any changes to their personal information
- Volunteers are responsible for informing their line manager of any changes to personal information (such as address, contact details). The line manager is then responsible for updating the internal records and removing any incorrect information.

Personal sensitive information will only be used for the exact purpose for which permission was given. In the case of user ethnicity, this information will only be used for collated, anonymised monitoring and evaluation purposes.

Data Security

Doorstep Library will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- Using lockable cupboards (restricted access to keys – employees only);
- Password protection on personal information files, restricted access to HR files and payroll system;
- Setting up computer systems to allow restricted access to certain areas;
- Employees working on personal computers, tablets or mobile phones must ensure no one else can access Doorstep Library files (including downloads),

passwords must be used and data deleted once no longer needed (delete downloads and empty recycle bin regularly. Don't save files except temporarily, then delete.)

- Passwords for Doorstep Library database and document cloud must not be auto-saved on tablets, laptops or mobile devices. Log out of computer account, email and database when leaving the computer.
- Ensure the computer has good virus protection. If needed Doorstep Library can purchase this.
- Paper copies of visit lists by Team Leaders - volunteers take these with them on visits but must return all copies to the Team Leader at the end of the session. Visit lists must be returned to the office for shredding.
- Volunteers are given access to Doorstep Library database (to access user information relating to the families they are to be visiting) only during project time. Volunteers are not to keep personal information relating to users, including contact details. The only exception is for Online Reading Volunteers who are required to save users' phone numbers for the purposes of their reading sessions. These must be anonymised and only used during project hours, strictly in accordance with rules laid out in Doorstep Library Volunteer Training and volunteer policy.
- Volunteers access the database using passwords that they set up, they must not disclose their password to anyone except DL employees;
- Any notes or written records of a sensitive nature should not be kept in the home of a volunteer (paper and electronic copies);
- Password protected attachments must be used for sensitive personal information sent by email;
- Bcc must be used for group emails to any recipients other than Doorstep Library employees, such as volunteers and families;
- Change your passwords immediately if you lose your mobile device/ laptop, or if you think your security may have been compromised.
- Passwords must always be kept confidential and not be disclosed to anyone outside of Doorstep Library, passwords must not be written down (on paper or electronically – unless they are held on a password protected file).

Any unauthorised disclosure of personal data to a third party, either by purpose or accident by:

- an employee - may result in disciplinary proceedings
- a trustee - may result in termination of trusteeship
- a volunteer - may result in the termination of the volunteering agreement

Any breach of data security will be reported to the Data Protection Authority within 72 hours of discovery, unless we are able to demonstrate that the breach is unlikely to result in any risk to data subjects.

Doorstep Library will notify affected data subjects if the breach is likely to result in a high risk to affected data subjects.

The breach will be logged and procedures reviewed. Depending on the severity of the breach the data protection policy may be updated to ensure against future breaches. Additional data security measures may also be put into place. Every effort will be taken to reobtain the lost/ disclosed data, and to encourage permanent deletion by the receiving party.

Data Retention

Doorstep Library will keep information for the following time periods:

- Applications for unsuccessful employee posts (and corresponding interview notes) – 1 year;
- Information on previous employees and trustees – 3 years;
- Information on previous volunteers – 3 years;
- Applications for unsuccessful volunteer posts – 1 year;
- Contact details (name, email, phone number, address) of supporters (donors, volunteers, interested parties) – for as long as they wish to remain on our mailing list – immediate removal from list and deletion of information on request;
- User information (personal details, user records (participation, case notes, referral forms)) – 6 years post participation for outcome assessment purposes.

Subject Access Requests

Anyone whose personal information we process has the right to know:

- What information we hold and process on them;
- How to gain access to this information;
- How to keep it up to date;
- What we are doing to comply with the Act/ Regulation.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as incorrect.

Individuals have a right under the Regulation to access their personal data. Any person wishing to exercise this right should apply in writing to the CEO or the Chair of the Board of Trustees

The following information will be required before access is granted:

- Full name and contact details of the person making the request;
- Their relationship with Doorstep Library (former/ current member of staff, trustee or other volunteer, service user).

We may also require proof of identity before access is granted.

In the case of excessive or manifestly unfounded access requests we may refuse or charge the person making the request. If we refuse a request for access, we will tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. We will do this without delay and at the latest, within one month of the request.

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible but will ensure it is provided within the 40 days required by the Act from receiving the written request.