DATA PROTECTION POLICY

Reviewed 20.1.21 by K.Millington

1. PURPOSE

1.1 Our Company Data Protection Policy refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

2. SCOPE

2.1 This policy applies to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to us.

3. DEFINITIONS

3.1 Data Controller – The person who, either alone or with others, decides what personal information The Open Doors Project CIC will hold and how it will be held or used.

3.2 General Data Protection Regulation (GDPR) 2018 – The EU legislation that that provides a framework outlining responsible behaviour for collecting, handling and storing personal information.

3.3 Data Protection Officer – The person(s) responsible for ensuring that The Open Doors Project CIC follows its data protection policy and complies with the General Data Protection Regulation (GDPR) 2018.

3.4 Data Subject/Service User - The individual whose personal information is being held or processed by The Open Doors CIC (e.g. service users, employees, volunteers, supporters, stakeholders).

3.5 Explicit consent – is a freely given, specific and informed agreement by a Data Subject to the processing of personal information about them. Explicit consent is needed for processing sensitive* data (* See definition below).

3.6 Notification – Notifying the Information Commissioner about the data processing activities of The Open Doors Project CIC, as certain activities may be exempt from notification.

3.7 Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the General Data Protection Regulation 2018

3.8 Processing – means collecting, amending, handling, storing or disclosing personal information.

3.9 Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as volunteers or employees within The Open Doors Project CIC.

3.10 Sensitive data – means data about:

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health

- Sexual life
- Criminal record or criminal proceedings relating to a data subject's offences

4. RESPONSIBILITIES

4.1 Everyone who works for or with The Open Doors Project CIC has some responsibility for ensuring that data is collected, stored and handled appropriately in line with data protection guidelines.

4.2 The Directors are ultimately responsible for ensuring that The Open Doors Project CIC complies with its legal obligations.

4.3 Data Controller – The Open Doors Project CIC is the Data Controller under the Act, which means that it determines the purpose for which personal information held will be used. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used.

4.4 The Data Protection Officer, currently Steffi Earle (Director) is responsible for:

- Briefing the Directors on Data Protection responsibilities;
- Reviewing Data Protection and related policies annually as agreed;
- Advising other staff on Data Protection issues, and ensuring that Data Protection training takes place;
- Notification;
- Handling subject access requests;
- Approving unusual or controversial disclosures of personal data;
- Approving contracts with Data Processors;
- Drawing up operational procedures (including induction and training) to ensure that good Data Protection practice is established and followed;
- Approving any data protection statements attached to communications such as emails and letters;
- Addressing any data protection queries including those from external media outlets;
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles;
- Approving any data statements attached to communications such as emails and letters;
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
- Ensuring regular checks and scans are carried out to ensure security hardware and software is functioning properly;
- Evaluating any third-party services the company is considering using to store or process data, for instance, cloud computing services.

4.5 The Directors are responsible for complying with this policy and to inform the Data Protection Officer of any changes in their use of personal data that might affect The Open Doors Project CIC Notification.

4.6 Data Processor - When work is outsourced and involves a contracting organisation having access to personal data, there must be a suitably written contract in place, paying particular attention to security. The Data Controller remains responsible for any breach of Data Protection brought about by the Data Processor

5. GUIDELINES

5.1 In order to ensure that there is no unauthorised or unlawful processing or disclosure of data, all data is:

- Fairly and lawfully processed;
- Obtained only for specific purposes as specified in the Act, and not processed in any manner incompatible with those purposes;
- Adequate, relevant, accurate and not excessive in relation to those purposes;
- Not kept for longer than is necessary;
- Processed in line with the Data Subject's rights under the Act;
- Not transferred outside the European Economic Area (EEA), unless that country or territory offers an adequate level of protection;
- Stored securely and kept by the Data Controller who takes appropriate measures to protect and prevent any unauthorised or unlawful processing or accidental loss, destruction or damage to personal information.

5.2 The Open Doors Project CIC will:

- Comply with both the law and good practice;
- Train and support staff and volunteers who handle personal data so that they can act confidently and consistently;
- Ensure only the people who need to access data for their work are the ones are granted access. Data will not be shared informally, internally or externally to non-authorised people;
- Respect individuals' rights, and be open and honest with individuals whose data it holds;
- Deal promptly and courteously with any enquiries about handling personal information;
- Allow the data subject to see the information on request;
- Ensure data is protected using strong passwords which are not circulated;
- Ensure that such data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects regarding the processing of personal information;
- Ensure data is regularly reviewed and updated and deleted or responsibly disposed of if no longer required or out of date;
- Give The Open Doors Project CIC service users clear information about why data is collected and how it is stored so that they can give informed consent
- Encourage staff to ask for help if unsure of their data protection responsibilities.

6. DATA COLLECTION

6.1 The data The Open Doors Project CIC collects and retains must be deemed necessary for the successful running of the organisation. Examples of the data we collect include service users' contact details, case notes, HR records or data needed to achieve organisational aims such as supporters' information.

6.2 Data may be held for the following purposes:

- Staff Administration
- Fundraising
- Realising the Objectives of a Charitable Organisation or Voluntary Body

- Accounts & Records
- Advertising, Marketing & Public Relations
- Research
- Volunteers

6.3 When collecting data, either in person or by completion of a form, The Open Doors Project CIC will ensure that the Data Subject

- Clearly understands why the data is needed and how it will be used;
- Understands the consequences why he/she decide not to give consent to processing;
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed;
- Understands that in certain circumstances, under the GDPR 2018, personal data may be disclosed to law enforcement agencies without the consent of the data subject;
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress.
- As these are legal requirements, it is important that The Open Doors Project CIC is open and honest with people about how their data will be used.

7. DATA STORAGE RULES

7.1 These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Controller.

7.2 When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. This also applies to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Staff should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

7.3 When data is stored electronically

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with The Open Doors Project's standard backup procedures.
- Personal information stored on portable devices, such as memory sticks and laptops must be appropriately encrypted and password protected.
- All servers and computers containing data should be protected by approved security software and a firewall.

- All personal and company data is non-recoverable from any computer system previously used within The Open Doors Project.

8. IT SECURITY

8.1 Data is stored on an encrypted hard drive, with 256-bit AES hardware encryption with WD security software. We also use Google Drive as our cloud based storage, which is 128-bit AES encrypted and requires a two-step verification to access data.

9. DATA TRANSMISSION

9.1 When data is transmitted as part of our services, care must be taken to protect our service users:

- The Open Doors Project CIC will offer a clear Informed Consent Process where information on services available and access to services is available via the website and in discussion with The Open Doors Project CIC staff;
- The Open Doors Project CIC will offer service users options about the method of communication they want to use to access our services;
- Methods of data transmission will be protected by strong passwords that are changed regularly;
- Interactions where data is transmitted will only take place via approved methods and platforms;
- Clients will be given clear information about the records The Open Doors Project CIC collects relating to its services.

10. DATA USE

10.1 Personal data is of no value to The Open Doors Project CIC unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

- When working with personal data, employees should ensure their computer screens are always locked when left unattended.
- Personal data should not be shared informally, and in particular, should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers, but always access and update the central copy of any data.
- Data should be held in as few places as possible and updated regularly.

11. DISCLOSURE

11.1 The Open Doors Project CIC may share data with other agencies such as the local authority, funding bodies and other voluntary agencies. The Data subject will be made aware in most circumstances how and with whom their information will be shared.

11.2 There are circumstances where the law allows The Open Doors Project CIC to disclose data (including sensitive data) without the data subject's consent. These are:

- Carrying out a legal duty or as authorised by the Secretary of State;
- Protecting vital interests of a Data subject or other person;
- The Data Subject has already made the information public;
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights;
- Monitoring for equal opportunities purposes – i.e race, disability, religion.

12. DATA ACCESS AND ACCURACY

12.1 All Data Subjects are entitled to:

- Ask what information The Open Doors Project CIC holds about them and why;
- Ask how to gain access to it;
- Be informed how to keep it up to date;
- Be informed how The Open Doors Project CIC is meeting its data protection obligations.

12.2 If an individual requests this information, they should complete a subject access request form before any information is handed over.

12.3 The Data Controlled will always verify the identity of anyone making a subject access request before handling over any information.

12.4 In response to a valid subject access request (including a fee, if required), the Data Controller will aim to provide the relevant data within 14 days.

12.5 The Data Controller may negotiate with the Data Subject to provide a more limited range of data (or may choose to provide more), and certain data may be withheld, including some third party material, especially if any duty of confidentiality is owed to the third party, and limited amounts of other materials. (Third party means either that the data is about someone else or someone else is the source.)

13. DISCLOSING DATA FOR OTHER REASONS

13.1 In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

13.2 Under these circumstances, The Open Doors Project CIC will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

14. TRAINING

14.1 Everyone processing personal data will appropriately be trained. New employees will receive Data Protection training as part of their induction to explain how they should store and handle personal information.

15. ENFORCEMENT

15.1 All staff must be aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

16. MONITORING AND REVIEW

16.1 The Open Doors Project CIC will regularly review and audit the ways personal information is held, managed and used, and evaluate its methods and performance in handling personal information.

16.2 This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the GDPR 2018.

16.3 In case of any queries or questions in relation to this policy, please contact The Open Doors CIC Project Data Protection Officer (Steffi Earle, Director).

17. LINKS WITH OTHER POLICIES

- Safeguarding Policy

Reviewed 20.1.21 by K.Millington