Charity Number 1175671

The Place- General Data Protection Regulation (GDPR) Policy

GDPR stands for General Data Protection Regulation and covers personal data relating to individuals that must be collected and used fairly, stored safely and not disclosed unlawfully.

Policy Statement
The Place needs to gather and use certain information about individuals. This includes anyone who is connected with the project, such as parents, children, staff, suppliers and business contacts. The Place must comply with data protection law and follow good practice, protect the rights of individuals connected with the project and explain how we store and process individuals' data. We will observe the six Privacy Principles:

- To have a lawful reason for collecting personal data and to do so in a fair and transparent way
- To only use data for the reason it was initially obtained
- To not collect any more data than is necessary
- To ensure any data we hold is accurate and that there are mechanisms in place to keep it up to date
- To not keep data any longer than needed
- To protect any data we hold

Rights for Individuals

The Right to be Informed:
The Place is required to collect, process and manage certain data.

The data we require is:

Trustees: Names, Addresses, Telephone Numbers, Email Addresses, Date of Birth

Employees: Names, Addresses, Telephone Numbers, Email Addresses, Date of Birth, National Insurance Numbers, Bank Details, Photographic I.D (Passport and Driving Licence), CVs This information is also required for Disclosure and Barring Service Checks (DBS) and proof of eligibility to work in the UK. The information is sent securely to *Due Diligence Checking Ltd* who complete the DBS checks with the information we provide to them, we then keep a record of the DBS number. We also require driving documents, eg license and insurance.

Partners, eg First Aid provider etc: Names, Addresses, Telephone Numbers, Email Addresses, Date of Birth, DBS certificate number

Volunteers: Names, Addresses, Telephone Numbers, Email Addresses, Date of Birth,Photographic I.D (Passport and Driving Licence). This information is also required for Disclosure and Barring Service Checks (DBS). The information is sent securely to *Due Diligence Checking Ltd* who complete the DBS checks with the information we provide to them.

Parents/Carers: Names, Addresses, Telephone Numbers, Email Addresses, Emergency Contact details

Children: Names, Addresses, Date of Birth
Medical Information, Accident records, Permission Forms, Routine forms

Visitors: Name, Company Name, Reason for Visiting The Place, Time Signed In, Time Signed Out and a Signature.

The Right of Access

At any point individuals can request to see their data, which The Place will respond to within 7 days. The request however can be refused, if we have a lawful obligation to retain data, but we will inform the individual of the reasons why. The individual will have the right to complain to the Information Commissioner's Office (ICO) if they are not happy with the decision.
https://ico.org.uk/

The Right to Restrict Processing

Any individual can object to The Place processing their data. This means that records can be stored but must not be used in any way.

The Right to Data Portability
Any individual can request the information they have provided us with and has the right to receive it in a structured, commonly used and machine readable format. They can also ask for this information to be transferred to another organisation.

The Right to Object:

Any individual can object to their data being used for certain activities, such as marketing or research. The Place may use photos from the project to put on our website or when making grant applications. However specific permission is sought from parents/carers and staff for this.

The Right Not to be Subject to Automated Decision Making*:*

The Place will always involve individuals in the decision making with regards to their data. We will not make a decision by automated means.

Storage and Use of Personal Data

All paper copies of children and staff records are kept in locked filing cabinets in the office. The office is also locked at night and over the weekends. Staff have access to the families' files; however these are kept in the office at all times in a locked filing cabinet. The information about individual children is confidential and the records remain on site at all times. Staff can request to see their own personal file at any time and will only have access to their own file. Staff and families' files are shredded after the retention period for records has passed. Information about individual children is used in certain documents, such as daily registers, medicine forms, accident books and referrals to external professionals. These documents include data such as children's names, date of birth and address. These records will be shredded after the retention period for records has passed. The Place collects personal data from families expressing an interest in the project, including names and contact details of those on the waiting list. These records are shredded if the family ends up not attending the project. Any information regarding a family's involvement with other agencies is stored safely on the office computer and is password protected and also in the child's file where one is required, which is in a locked cabinet in the office. These records are shredded after the retention period for records has passed. When a family stops using the project personal data will be shredded after any retention period has passed. The Place may take photos of children that have been taken with parental/guardian consent which will be stored on the main office computer, which is password protected. These photos may be used on the website or in grant applications or reports. We will obtain specific consent for any such use. Access to the office computer, staff laptop and staff tablets is password protected. USB sticks should not be used.

In determining the time periods for retention of documents we use the legal ombudsman's guidelines which can be found at https://www.legalombudsman.org.uk/

Third Party Sharing and Processing

The Place may need to share personal data for specific purposes with outside agencies or organisations. We refer to these as 'third parties'. This may be for a variety of reasons but where this is necessary The Place will ensure all third parties who process data on our (the data controller's) behalf have robust systems in place to comply with the conditions set out in GDPR. The Place will seek consent for sharing of information for such purposes, for example employee details for processing our payroll. Personal data is only disclosed to third parties outside a formal contract or agreement where there is a legal obligation to do so, such as safeguarding a child or adult.

Roles and Responsibilities

All Members of staff who work for The Place have a responsibility to ensure that data is collected, stored, processed and disposed of appropriately. The Trustees are responsible for ensuring that appropriate policies are in place. The Manager is responsible for ensuring that policies are implemented and data protection guidelines are adhered to.

Data Protection Risks

Everyone at The Place has a responsibility for ensuring data is collected, stored and handled appropriately. However there are always risks that come with data protection. These could be:

- Breaches of confidentiality – If any information is given out inappropriately
- Not offering choice – all individuals should be free to choose how The Place uses data relating to them
- Reputational Damage – Any information that is successfully gained by hackers or a break in

Complaints

If any individual has concerns about the way The Place handles, processes and stores data please raise it with the management team. Alternatively you can contact the International Commissioner's Office (ICO): Telephone Number: 0303 123 1113 Web Address: https://ico.org.uk/concerns/

Appendix 1

General Staff Guidelines

All employees of The Place are required to comply with the following guidelines to ensure all personal data held by the project is used, stored and managed in the most appropriate way possible:

- Data should only be collected on approved Place documentation - eg application forms
- Data should only be used for its original purpose and only by those who need it for their work
- Data concerning individuals must not be communicated to other persons or organisations unless required to do so by law or under an approved contract
- Care should be taken when sharing data that you have checked the identity of the individual and the organisation they are representing and you are confident they have a legitimate need for the information

- Take sensible precautions to ensure all personal data is kept secure. This should include locking computers when leaving a desk and making sure no personal data is left out in view of other people.
- Use strong and secure passwords when storing digital data and usernames and passwords should never be shared
- Data should be regularly reviewed and updated, and if found to be out of date or no longer required for its original purpose, it should be updated or deleted and disposed of securely.
- Employees should request help from the manager or designated trustee if they are unsure of any aspect regarding data protection
- Documents containing personal data should be disposed of by shredding on site. Documents that contain personal data should not be placed in general waste bins.
- The Place will provide training to all employees to help them understand their responsibilities when handling data
- Employees should ensure that the data held on HR software is reviewed at least annually and updated

Staff that work from home or carrying out activities at other activities, e.g Faringdon Library, Ferendune etc. should comply with the following guidelines:

- Only use a laptop or tablet that has been installed with approved firewall and security software
- Documents that include personal data should be worked on only an official laptop or tablet belonging to The Place and should not be downloaded and saved to personal computers or hardware
- Data should not be transferred onto a personal USB stick
- Employees should avoid leaving sensitive information out on display or in vehicles
- Computers and tablets should be password protected and locked when left unattended
- Documents containing personal data that are no longer required should be taken back to the office to be shredded; they should not be placed in a general waste bin.

Appendix 2

Related policies and documents:

- Privacy Notice
- Social Media Policy
- Photo Policy

This document has been drawn up using guidance from:

https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/data-protection-tips-for-early-years-settings/

https://assets.publishing.service.gov.uk/media/6641db10b7249a4c6e9d32d4/SSRO_Retention_and_Disposal_Policy.pdf

https://www.legalombudsman.org.uk

https://www.eyalliance.org.uk/early-years-settings-and-gdpr

As advised by the ICO in October 2024, there is no requirement for The Place to be registered with them.

Policy adopted	November 2024
Review Date	November 2025

JMC 10/24