Privacy Standard Policy

Policy created	01.06.2018	Version number	1.0
Last reviewed	01.11.2026	Next review date	01.11.2027

General

This Privacy Standard sets out how the Pre-school handles the personal data of children, parents of children, suppliers, employees, volunteers and other third parties. It applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present children in setting (and their parents), employees, volunteers or supplier contacts, shareholders, website users or any other data subject.

This Privacy Standard applies to all Pre-school employees. Pre-school employees are required to read, understand and comply with this Privacy Standard and our Privacy Notices when processing personal data on our behalf and attend training on its requirements as available. This Privacy Standard sets out what we expect from you for the Pre-school to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Any breach of this Privacy Standard or our Privacy Notices may result in disciplinary action.

This Privacy Standard (together with the Privacy Notices) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Chairperson.

Scope

We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will contribute to the successful operation of our Pre-school. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. The Pre-school is exposed to potential fines for failure to comply with the provisions of the General Data Protection Regulation/Data Protection Act 2018 (collectively **GDPR**).

The Committee and Setting Manager are responsible for ensuring all employees comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The Committee are responsible for overseeing this Privacy Standard and, as applicable, developing related policies guidelines. The Committee may delegate specific responsibility to individual members from time to time.

Please contact the Chairperson with any questions about the operation of this Privacy Standard or the GDPR or if you have any concerns that this Privacy Standard is not being or has not been followed.

Personal data protection principles

We adhere to the principles relating to processing of personal data set out in the GDPR which require Personal Data to be:

- processed lawfully, fairly and in a transparent manner;
- collected only for specified, explicit and legitimate purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and where necessary kept up to date;
- not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed;
- processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage;
- not transferred to another country without appropriate safeguards being in place; and
- made available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data.

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

Lawfulness, fairness, transparency

Personal data must be processed lawfully, fairly and in a transparent manner.

We will only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject.

The GDPR allows processing for specific purposes, including:

- the data subject has given his or her consent;
- the processing is necessary for the performance of a contract with the data subject;
- to meet our legal compliance obligations.;
- to protect the data subject's vital interests;
- to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

The purposes for which we process personal data are set out in our separate Privacy Notices in relation to each processing activity. The Privacy Notices include all the information required by the GDPR including the identity of the data controller (Plymtree Pre-school) and how and why we will use, process, disclose, protect and retain personal data.

If we rely on consent to process personal data, we will keep a record of any consent given to demonstrate our compliance with the requirements of the GDPR in relation to consent. Data subjects may withdraw consent to process data and that withdrawal will be promptly honoured provided it is not overridden by a legal obligation placed upon Pre-school.

Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. We will not use personal data for new, different or incompatible purposes from those set out in our Privacy Notice or when the personal data was first obtained unless we have informed the data subject of the new purposes and our legal basis for processing.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

We will only process personal data in fulfilling the duties and responsibilities of Pre-school. We will not process personal data for any reason unrelated to Pre-school. Any personal data which is collected will not be excessive and will be adequate and relevant for the intended purposes.

We will ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised.

Accuracy

Personal data kept by Pre-school must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We will take reasonable steps to ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. 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 or out-of-date personal data.

Storage limitation

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

We will not keep personal data in a form which permits the identification of the data subject for longer than needed for the purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

We will ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

We will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all the Company's applicable records retention schedules and our policies and legal and regulatory obligations. We will inform data subjects of the period for which data is stored and how that period is determined in our Privacy Notices.

Security integrity and confidentiality

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our setting, our available resources, the amount and type of personal data that we own or maintain on behalf of others and identified risks. We will regularly evaluate the effectiveness of those safeguards to ensure security of our processing of personal data. We will implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. We will exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

We will only transfer personal data to third-party service providers who agree to put adequate measures in place, as requested.

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

- We will ensure that only people who have a need to know and are authorised to use the personal data can access it (**confidentiality**).
- We will ensure that personal data is accurate and suitable for the purpose for which it is processed (**integrity**).
- We will ensure that authorised users are able to access personal data when they need it for authorised purposes (**availability**).

Reporting a Personal Data Breach

The GDPR requires data controllers to notify any personal data breach to the applicable regulator and, in certain instances, the data subject.

We will notify data subjects or any applicable regulator of a personal data breach where we are legally required to do so.

If an employee or committee member knows or suspects that a personal data breach has occurred, should not attempt to investigate the matter themselves but should immediately contact the Chairperson. All evidence relating to the potential personal data breach should be preserved.

Transfer limitation

We do not transfer personal data outside the EEA (European Economic Area).

Data subjects' rights and requests

Data subjects have rights when it comes to how we handle their personal data. These rights are set out in our Privacy Notices.

We will verify the identity of an individual requesting data under any of the rights listed in the Privacy Notice.

Any data subject request received should be forwarded immediately to the Chairperson.

Accountability

Data controllers must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

Record keeping

The GDPR requires us to keep full and accurate records of all our data processing activities.

We will keep and maintain accurate records reflecting our processing including records of data subjects' consents and procedures for obtaining consents.

Our records will include the name and contact details of the Pre-school and the individual to whom any queries should be addressed, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

Training and audit

We will ensure that, where appropriate, staff and committee members receive adequate training to enable them to comply with data privacy laws.

We will regularly review all the systems and processes under our control to ensure they comply with this Privacy Standard and check that adequate controls and resources are in place to ensure proper use and protection of personal data.

Sharing personal data

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

We will only share the personal data we hold with employees and committee members if the recipient has a job/setting-related need to know the information.

We will only share the personal data we hold with third parties in line with our E-Safety Policy and only if:

- the recipient has a need to know the information for the purposes of providing contracted services;
- sharing the personal data complies with the Privacy Notice provided to the data subject and, if required, the data subject's consent has been obtained; and
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place.

Applicable law

This Privacy Standard does not override any applicable national data privacy laws and regulations in England and Wales.

The following legislation contains provisions dealing with data protection:

- **Computer Misuse Act 1990**
- **Regulation of Investigatory Powers Act 2000**
- **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**
- **Privacy and Electronic communications (EC Directive) Regulations 2003**
- **General Data Protection Regulation**
- **The Data Protection Acts**

Related policies

The following policies and procedures are relevant to data protection and confidentiality and must be considered when complying with this policy:

- E-Safety policy
- Funding & Payment policy
- Registration policy
- Safeguarding policy

Document History

Date	Change details	Reviewed by

04/07/18	New policy created	Ellie Hibberd
02/10/18	Policy reviewed – no updates	Donna Manser
01/10/19	Policy reviewed – no updates	Donna Manser
23/10/20	Policy reviewed – no updates	Anna Shelbourne
22/09/21	Policy reviewed – no updates	Anna Shelbourne
29/09/22	Policy reviewed – no update	Anna Shelbourne
01/09/23	Policy reviewed – no update	Charlotte Gibbins
01/09/24	Policy reviewed- no update	Charlotte Gibbins
01/10/25	Policy reviewed – no update	Clare Livingstone
01/11/26	Policy reviewed – no update	Clare Livingstone