General Data Protection Regulation (2018) POLICY

Policy statement

The General Data Protection Regulation (GDPR) is a new EU law coming into effect on 25th May 2018 replacing the current Data Protection Act 1998. It will give individuals greater control over their own personal data. As a nursery it is necessary for us to collect personal information about the children who attend as well as staff and parents/carers.

GDPR principle

GDPR condenses the Data Protection Principles into six areas, which are referred to as the Privacy Principles. They are:

1. You must have a lawful reason for collecting personal data and must do it in a fair and transparent way.
2. You must only use the data for the reason it is initially obtained.
3. You must not collect any more data than is necessary.
4. It has to be accurate and there must be mechanisms in place to keep it up to date.
5. You cannot keep it any longer than needed.
6. You must protect the personal data.

The GDPR provides the following rights for individuals:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erase.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision-making and profiling.

There are two main roles under the GDPR; the data controller and the data processor. As a childcare provider, we are the data controller. The data is our data that we have collected about the children and their families. We have contracts with other companies to process data, which makes them the data processor. The two roles have some differences but the principles of GDPR apply to both. We have a responsibility to ensure that other companies we work with are also GDPR compliant.

Lawful basis for processing personal data

We must have a lawful basis for processing all personal data within our organisation and this is recorded on our Information Asset Register for all the different information we collect. The six reasons are set out in Article 6 of the GDPR as follows:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

For the majority of data we collect, the lawful basis for doing so falls under the category of 'legal obligation' such as names, date of birth and addresses as we have a legal requirement to obtain this data as part of the Statutory Framework for the Early Years Foundation Stage. Some data we collect, for example, photographs, requires parents to give consent for us to do so. Where this is the case, parents will be required to sign a consent form to 'opt in' and are made aware that they have the right to withdraw their consent at any time.

We may also be required to collect data as part of parent's contract with the setting or local authority, for example, in order for us to claim government funding.

Data retention

We will hold information about individuals only for as long as the law says and no longer than necessary. After this, we will dispose of it securely. Please see (Information Asset Register) for more information on retention periods for individual documents.

Security

We keep data about all individuals secure and aim to protect data against unauthorised change, damage, loss or theft. All data collected is only accessed by authorised individuals. All paper forms are kept locked away and all computers and tablets are password protected.

Privacy notices (appendix ii. and iii.)

All parents and staff are provided with privacy notices which inform them of our procedures around how and why we collect data, information sharing, security, data retention, access to their records and our commitment to compliance with the GDPR act.

Ensuring compliance

The member of staff responsible for ensuring that the setting is compliant is Sarah Kelly (Company Director/Manager). Their main duties are:

- Ensure that the provision is compliant with GDPR.
- Audit all personal data held.
- Establish an Information Asset Register and maintain it.
- Ensure all staff are aware of their responsibilities under the law, this may include delivering staff training.
- Undertake investigations when there is a breach of personal data and report to the ICO.
- Keep up to date with the legislation.

The setting is also registered with the Information Commissioners Office and the certificate can be viewed in the office.

Data breach

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed. Recital 87 of the GDPR makes clear that when a security incident takes place, we must quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Where there has been a personal data breach, the person responsible for monitoring the setting's GDPR compliance will complete the Data Breach Reporting Form within 72 hours.

Legal framework

- The General Data Protection Regulation (2018)
- Human Rights Act 1998

Policy created: May 2018 **by:** Sarah Kelly (Director and Nursery Manager)

Signed:

The policy will be reviewed **annually** from the above date (Please see separate review sheet in office policy folder). Any policies which require changes (at or in between review dates) will be updated and communicated to all employees, parents and students/volunteers