



GENERAL DATA PROTECTION REGULATION POLICY

Statement of Intent

The General Data Protection Regulation (GDPR) is designed to protect the privacy of individuals. It requires that any personal information about an individual is processed securely and confidentially. This includes both staff and children. How the pre-school obtains, shares and uses information is critical, as personal data is sensitive and private. Everyone, adults and children alike, has the right to know how the information about them is used. The General Data Protection Regulation requires the pre-school to strike the right balance in processing personal information so that an individual's privacy is protected. Applying the principles to all information held by the pre-school will typically achieve this balance and help to comply with the legislation.

We will respect the privacy of children and their parents and carers, while ensuring that they access high quality early years care and education in our setting. We aim to ensure that all parents and carers can share their information in the confidence that it will only be used to enhance the welfare of their children. There are record keeping systems in place that meet legal requirements; means of storing and sharing that information take place within the framework of the General Data Protection Regulation and the Human Rights Act.

General Data Protection Regulation principles

To comply with the act, the pre-school must observe the eight 'General Data Protection Regulation principles', ensuring that:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal 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 in relation to the processing of personal data.

In practice, it means that the pre-school must:

- have legitimate grounds for collecting and using the personal data;

Policy and Procedures

Updated Sept 08; Feb 09, Oct 13, Jan 16, Oct 17



- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure they do not do anything unlawful with the data

Personal data is information that relates to an identifiable living individual that is processed as data. Processing amounts to collecting, using, disclosing, retaining or disposing of information. The General Data Protection Regulation principles apply to all information held electronically or in structured paper files.

The principles also extend to educational records – the names of staff and children, dates of birth, addresses, national insurance numbers, school marks, medical information, SEN assessments and staff development reviews.

Sensitive personal data is information that relates to

- race and ethnicity,
- political opinions,
- religious beliefs,
- membership of trade unions,
- physical and mental health,
- sexuality
- criminal offences

Sensitive personal data is given greater legal protection as individuals would expect certain information to be treated as private or confidential – for example, a pre-school manager may have a pre-school e-mail account that is made publicly available on the school's website whereas their home e-mail account is private and confidential and should only be available to those to whom consent had been granted.

It is important to differentiate between personal information that individuals would expect to be treated as private or confidential (whether or not legally classified as sensitive personal data) and personal information you can make freely available. For example: the pre-school manager's identity is personal information but everyone would expect it to be publicly available. However, the pre-school manager's home phone number would usually be regarded as private information.

What must the pre-school do?

- We must notify the ICO (Information Commissioner's Office) that we are processing personal data.
- We have a nominated individual, the Pre-school Director, as the 'Data Protection Controller'.
- The pre-school has clear, practical policies and procedures on information governance for staff to follow, and needs to monitor their operation
These should include:
 - Staff Code of Conduct
 - Privacy notices for staff and parents/pupils
 - Record Management Policy (not mandatory, but good practice)

Policy and Procedures

Updated Sept 08; Feb 09, Oct 13, Jan 16, Oct 17



Data Breaches – In the event of a personal data breach, the Data Protection Controller should be notified immediately and an investigation carried out.

Individual Rights

The General Data Protection Regulation includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

The General Data Protection Regulation entitles an individual the right to request the personal information a pre-school holds on their behalf – this is known as a Subject Access Request (SAR) and includes all and any information held by the pre-school, not just that information held on central files or electronically, so it could also include correspondence or notes held by others in the pre-school.

- SARs must be responded to within 1 month of receipt.
- The SAR should be made in writing by the individual making the request.
- The pre-school can refuse or charge for requests that are manifestly unfounded or excessive
- Parents can make SARs on behalf of their children if the children are deemed to be too young or they have consented to their parents doing so on their behalf.

Staff Responsibilities

Staff need to know and understand:

- How to manage, keep and dispose of data
- The pre-school's procedures in relation to children's records, email, social media, taking photos in the pre-school, mobile technology and the pre-school website
- When they are allowed to share information with others and how to make sure it is kept secure when shared.

Access to staff personal data

- Employees are allowed to have access to all personal data about them held on manual or computer records under the Data Protection Act (1998). The Act requires the organisation to action requests for access to personal data within 40 days.
- Should an employee request access to their personal data, the request must be addressed in writing to the relevant line manager. The request will be judged in the light of the nature of the personal data and the frequency with which they are updated. The employee will be informed whether or not the request is to be granted. If it is, the information will be provided within 40 days of the date of the request.

Policy and Procedures

Updated Sept 08; Feb 09, Oct 13, Jan 16, Oct 17



- In the event of a disagreement between an employee and the line manager regarding personal data, the matter should be taken up under the charity's grievance procedure.
- The right of employees to see information held about them is extended to information held in paper record-keeping systems as well as computerised systems.
- There are some exemptions; for example employees will not be able to see employment references about them supplied in confidence, nor will people involved in negotiations with the data controller be able to see information about the data controller's intentions in relation to those negotiations.
- Employee data cannot be used for direct marketing (including fundraising) if the data subject objects. Approval to use employee data for marketing purposes must be sought from the Director of Communications.

Legal Framework

General Data Protection Regulation 2018 <https://ico.org.uk/>

Data Protection Act 1998

Freedom of Information Act 2000

Human Rights Act 1999

The Children Act 2004, 2006 (Every Child Matters)

Statutory Framework

Statutory Framework for the Early Years

Section 3: The Safeguarding and Welfare requirements 3.67-3.72

Guidance

Please see separate Child Protection Policy.

Adopted at staff meeting.....
Date.....
Review Date.....

Policy and Procedures

Updated Sept 08; Feb 09, Oct 13, Jan 16, Oct 17