GENERAL DATA PROTECTION REGULATIONS (GDPR)

User Terminology

Data Subject:	Parents and children
Data Controller:	Frances Carr, Owner/Manager (the person who controls how the information is processed)
Data Processors:	All permanent employees of the preschool service

Types of Data

1. Personal Data:

Any information relating to an identified or identifiable Data Subject

Examples:

- Name
- Address
- Phone number
- Email address
- IP address
- Passwords

(e.g. the doctor's mobile number is sensitive data, his surgery number is not)

2. Sensitive Data:

Personal data revealing facial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

Examples:

- Behavioural characteristics
- Health/genetic data
- Facial images (i.e. photos)

Data Subjects' Rights

- Right of Access (Data Controller must respond within 30 days)
- Right of Rectification (corrections)
- Right of erasure ('right to be forgotten')
- Right to compensation and redress

Any requests under the above rights must be made in writing to the Data Controller (the owner/manager).

Enforcement

Office of the Data Protection Commissioner (ODPC).

Definition of a Data Breach

A data breach is not specifically defined in the regulations.
Controllers/processors must protect personal data against accidental or unlawful destruction, or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing.

Handling of a Data Breach/Reporting Obligations

The ODPC must be notified within 72 hours of a data breach. This notification must include details of the breach, the number of Data Subjects affected, the impact of the breach, and any containment and/or mitigation measures made by the Data Controller/Processors to secure the data against such a breach again.

Examples of a Data Breach

- Lost data
- Text or email sent to the wrong parent

Consequences of a Data Breach

- Reputational damage
- Time cost in assisting investigation
- Possibility of an investigation by the ODPC
- Fines levied by ODPC
- Potential for being sued by Data Subject

Access to Data

(The following list is an indication of the type of individuals/organisations that may access data, although this list is not exhaustive)

- Data Controller
- Data Processors
- Túsla
- Pobal
- Department of Education and Skills
- Department of Children and Youth Affairs
- An Garda Síochána
- South Dublin County Childcare Committee
- Banks (e.g. employee salaries, payment of school fees)
- Accountants/book-keepers
- Human Resource support
- IT support
- Legal support

How Data will be Collected

- Enrolment Form
- Medical Records Form

- Personal communication with Parents/Authorised Minders
- Personal requests to Parents
- Ad hoc permissions may be sought throughout the school year.

Why Data will be Collected and Processed

The data collected will be used to assist teachers in helping to make your child's time at preschool as safe and comfortable as possible.

Data Storage

- Data will be stored in a locked filing cabinet in the service.
- The key will be available to all permanent employees of the service (Data Processors) during school hours.
- The key will be kept in a place agreed by the owner (Data Controller) and employees (Data Processors), out of sight and not next to the locked filing cabinet, while the school is closed.
- All school access doors and windows (front and rear) will be locked at all times outside school hours.

Retention Periods for Data

Child's Data:	Two years after leaving the service
Garda Vetting forms:	Five years
Financial Information:	Six years
Discipline/Grievance:	Six years, or as advised by insurance company or solicitor