EY Service***

DATA PROTECTION POLICY

Document Status and Issue Control:

Version: 3

Date: January 2021

Contents Page No.

INTRODUCTION

Why This Policy Exists

EY Service*** (hereafter referred to the "Service") needs to gather and use certain information about individuals.

These can include parents/guardians, children, clients, suppliers, business contacts, employees, and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled, and stored to meet the organisation's data protection standards — and to comply with the law.

The purpose of this document is to explain to staff and employees what can and cannot be done with this information and **forms an essential part of awareness training for all staff.**

This data protection policy ensures that the Service:

- Complies with data protection law and follow good practice,
- Protects the rights of staff, clients and partners,
- Is open about how it stores and processes individuals' data, and
- Protects itself from the risks of a data breach.

See also the policy on the use of the Internet and Photographic and Recording Devices in main policy document as required under the Child Care Act 1991 [Early Years Services] Regulations 2016.

Safeguarding Against Data Protection and Security Risks

This policy helps to protect the Service from some very real data security risks, including:

- **Breaches of security and confidentiality.** For instance, information being given out inappropriately.

- **Reputational damage.** For instance, the Service could suffer if hackers successfully gained access to sensitive data.
- The risk of **large fines** or sanctions being imposed by the authorities.
- The **risks of being sued** for damages by individuals whose data has been mishandled.

DATA PROTECTION LAW AND CORE PRINCIPLES

The Laws

The Data Protection Acts of 1988-2018 (the "Data Protection Acts") incorporate the 2016 General Data Protection Regulations ("GDPR"). The Acts describe how organisations including our Service must collect, handle, and store personal information.

These rules apply regardless of whether data is stored electronically, on paper, or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely, and not disclosed unlawfully.

The Data Protection Acts and the GDPR are underpinned by eight important principles. These, and a description of how they are implemented within the Service, are described below.

The Principles - Management of Personal Data

All personal data collected and held by the Service must be managed strictly within the eight guiding principles as set out in the GDPR. **Personal Data must be:**

- **Processed Fairly and Lawfully**

At the time we collect information about individuals, they are made aware of the uses for that information. Where information is disclosed to third parties, this is also set out and explained. This information is set out in the Service's **Privacy Notices.**

- **Processed Only for Specific Lawful Purposes**

Personal information is only kept for clearly described and explicit purposes. The types of information retained and the specific purposes it is used for and details of any third-party disclosures are set out in the Service's **Register of Personal Data Records.**

- **Adequate, Relevant, and Not Excessive**

The Service collects sufficient information to provide an early childhood care and education service to children and their families. The data collected is set out in our Privacy Notices and Register of Personal Data Records.

- **Kept Accurate and Up-to-Date**

The personal data that the service collects is checked for accuracy at the time of first collection, and the data subjects (e.g. parents, guardians, staff and others) are given the opportunity to update information freely whenever they are in contact with the service over the duration of the period that they attend (children, parents. Guardians) or work in the service (staff).

Personal information is retained for such time as required to provide the required services to staff and clients - or to comply with the relevant industry standards, legal requirements or guidelines. These are set out in detail in the Service's **Personal Data Register with the associated retention guidelines.** Once data has reached the retention threshold, it will be authorised for secure disposal and/or deletion.

- **Processed in Accordance with the Rights of Data Subjects**

Where staff or clients wish to exercise their subject rights in terms of Data Access, correction, or erasure this will be honoured as set out in the Service's **Subject Access Request handling procedure.**

- **Kept Secure and Protected in Appropriate Ways**

All personal information held within the Service is kept securely, and protected as described below under Information Security Guidelines, and set out in more detail in the Service's **Information Security Overview** document.

- **Protected Against Transfer to Countries Without Adequate Safeguards**

No personal data is currently transferred outside the European Economic Area (EEA). If this ceases to be the case, appropriate measures will be taken to ensure the necessary safeguards are put in place and that the target country or territory can guarantee an adequate level of protection

Personal Data and Handling of Special Categories (Sensitive) Personal Data

Personal Data

Under GDPR, '**Personal Data**' means any information relating to an identified or identifiable natural person ('data subject').

In other words, any information that is clearly about a particular person. In certain circumstances, this could include anything from someone's name to their physical appearance.

The definition is wide ranging but typically within the child-care environment would include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Photographs
- PPSN numbers
- Staff and Parent's Bank Account details

and any and all other information relating to individuals.

Payment data

Payment data refers to your payment details such as the IBAN, BIC and the name of your bank/building society which will be collected by the Organisation and processed by us in the event that you purchase from our website or receive payments through electronic fund transfers.

Digital Platforms

When you interact with the Organisation's digital platforms/website you will often provide personal data to the Organisation which you will be aware of when using the services. The Organisation automatically collects data about your use of its services such as the IP address of the device you use to access the service, the type of device you are using and how you interact with the services.

Special Categories of Personal Data

This is a particular set of sensitive data that can only be collected and used if specific conditions have been met and which must be treated with extra security. The categories are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data (where processed to uniquely identify someone);
- Data Concerning health; or
- Data concerning a natural person’s sex life or sexual orientation.

Under GDPR, processing of these special categories of information is prohibited unless certain conditions have been met.

Within the Early Years environment this means that **you must obtain explicit consent from the data-subject** - i.e. the staff member, or parent/guardian(s) - in each case.

You must take care to obtain this consent at the time an employee first joins the Service or when a parent/guardian or parents/guardians register their child using the appropriate application or registration forms.

The records of consent should be retained securely for the periods recommended in the **Data Retention Procedure [i.e as outlined in the Data Retention Form Appendix VIII.**

RESPONSIBILITIES AND COMPLIANCE

Policy Scope

Everyone who works for or with the Service has responsibility for ensuring data is collected, stored, and handled appropriately. Each person that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. Specific responsibilities are outlined in more detail below.

Management

Persons with responsibility for the implementation of the policy are as follows:

Manager: Nina Patterson
Data Controller: Ciara Watson and Kara Gargolinski Mc Alister
Child Protection : Ciara Watson and Kara Gargolinski Mc Alister

- Management will ensure that the basic principles of data protection are explained to staff and parents/guardians. This will be done during staff

induction, staff meetings and if possible, through the Service's parent handbook/notice board.

- There are regular updates to data protection awareness, so that data protection is a “living” process aligned to the way the service conducts its business.
- The Data Controller will periodically check data held regarding accuracy and will complete regular security reviews.
- Non-compliance of the data protection and other policies of the Service may invoke the disciplinary policy and procedure.
- Confidential and personal information about the Service's children, parents or guardians, and staff will only be shared by Management, Data Controllers, and Designated Child Protection Liaison Persons in relation to child safety, in line with our Child Protection Policy and Safeguarding Statement. Any breach of confidentiality by any member of staff will lead to disciplinary action.

The Data Controller (see designated person above)

To ensure the implementation of this policy, the Service has designated a Data Controller. All enquiries relating to the holding of personal data should be referred to the Data Controller in the first instance.

The Data Controller will:

- Inform the person or persons involved a breach of confidentiality has occurred and their personal data may have been compromised. A record of this will be kept on the employee’s file or child’s file as relevant.
- Investigate where the breach of security has occurred and invoke the disciplinary policy if necessary.
- Check that additional measures are in place to ensure confidentiality.
- Review and update the Data Protection Policy if required.
- Check that any information kept is necessary for running the Service.
- Check to see if clerical and computer procedures are adequate to ensure accuracy.

- Reassure parents/guardians that the Data Protection Policy has been reviewed and additional measures to ensure security.
- Advise and inform employees of the need to ensure confidentiality through additional staff training and re-implementation of the Data Protection Policy.

Employees will be required to sign off to confirm they have read and understand the Data Protection Policy and Procedures.

Employees Responsibilities

As an employee, you are responsible for:

- Checking that any information that you provide in connection with your employment is accurate and up to date.
- Notifying the Service of any changes to information you have provided, for example changes of address.
- Ensuring that you are familiar with and follow the Data Protection Policy.
- Ensuring that any personal data you hold, whether in electronic or paper format, is kept securely.
- Personal information relating to children or their families is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.

Sanctions and Disciplinary Action

Given the serious consequences that may arise, the Service may invoke the disciplinary policy and procedure in relation to employees. Sanctions include warnings up to and including dismissal for breaching the rules and guideline on data.

In the case of contractors or external service providers, serious breaches of the policies and procedures can and will be deemed grounds for termination of contractual agreements.

Any breach of the data protection policy, either deliberate or through negligence, may lead to disciplinary action being taken and could in some cases result in a criminal prosecution.

Compliance Monitoring and Review

The Service will undertake regular reviews of the internal operation and changes in the legislation to ensure ongoing compliance with Data Protection Regulation. These will comprise of an annual review.

INFORMATION SECURITY - GENERAL GUIDELINES

Overview

- Access to the information should be restricted to authorised staff on a "need-to-know" basis and where data is needed to carry out their job descriptions.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from management (as outlined above in this policy).
- The Service will provide training to all employees to help them understand their responsibilities when handling data.

- Employees should keep all data secure by taking sensible precautions and following the guidelines below.
- Strong **passwords must be used,** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the Service or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their manager or the Data Controller if they are unsure about any aspect of data protection.

Data Storage

The security of personal information relating to children and families is a very important consideration under the Data Protection Acts. Appropriate security measures will be taken by the Service to protect unauthorised access to this data and to the data it is collecting and storing on behalf of the DCYA.

A minimum standard of security will include the following measures:

- Access to the information should be restricted to authorised staff on a "need-to-know" basis. Management will assign responsibilities regarding data at induction. Authorised staff are those identified by management and made known to such staff.
- Manual files will be stored in a lockable filing cabinet located away from public areas.
- Computerised data will be held under password protected files with a limited number of authorised staff.
- Any information which needs to be disposed of will be done so carefully and thoroughly.
- The Service's premises has the following security arrangements: All files are kept in a locked filing cabinet and the Data Controller retains the key to same.

If you have any questions or concerns about where or how to store data, please refer to the manager or data controller as outlined above.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them** (for example, parents should not have access or see other parents' names/phone numbers).
- **Data should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (e.g. a CD or USB key device), these should be kept locked away (and ideally encrypted) when not being used.
- Data should be stored on **designated drives and servers** and should only be uploaded to **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**.
- Data should be **backed up frequently**. Those backups should be tested regularly in line with the Service's standard backup procedures.
- All servers and computers containing data should be protected by an **approved security software and a firewall**.

Data Use

Personal data is at often at the greatest risk of loss, corruption, or theft when it is being used or accessed:

- When working with personal data, employees should ensure **the screens of their computers/tablets/apps are always locked** when left unattended.
- Personal data **should not be shared informally.**

- Personal data shared by email should be **downloaded, stored securely, and then deleted.**
- Data must be **encrypted before being transferred electronically.**
- The manager can explain how to send data to authorised external contacts.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data Accuracy

The law requires the Service to take reasonable steps to ensure data is kept accurate and up-to-date.

The more important it is that the personal data is accurate, the greater the effort we will put into ensuring its accuracy. It is the responsibility of all employees who work with data to take all reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated** (for instance, by updating parent's contact information).
- The Service will make it **easy for data subjects to update the information** held about them, over the phone, or by email.
- Data should be **updated as and when inaccuracies are discovered**. For instance, if a member can no longer be reached on their stored telephone number, it should be removed from the database.

Data Disclosure to Third Parties

As the Data Controller, the Service is ultimately responsible for any personal data passed to third parties and care must always be given to procedures and security.

The only data disclosed to third parties in the normal course of events is as described in the Service's Privacy Notices and Register of Personal Data Records.

In certain circumstances, the Data Protection Acts allow personal data to be disclosed to external agencies without the consent of the data subject. Any requests from external bodies and agencies not specifically provided for in legislation including An Garda Síochána, should be in writing.

Under these circumstances the Service will disclose requested data; however, the Data Controller must ensure the request is legitimate, seeking assistance from Management and from the Service's legal advisers where necessary.

Please note that information may need to be disclosed to authorised third parties. The Service will always check validity of any requests made.

The following list includes examples of such organisations but is not exhaustive:

- An Garda Síochána
- Early Years Inspection Team
- DES Inspection Team
- Pobal Compliance Officers
- DCYA and Childcare Committees
- Insurance Company
- Health and Safety Authority
- Workplace Relations Commission
- Revenue Commissioners
- HR Advisors
- Other Professional Advisors

Please note that where information may need to be disclosed to authorised third parties, **it is essential to always check validity of any requests** made before release of the data.

Note: Data Collected Through Garda Vetting

The Service understands that sensitive information may be identified through Garda Vetting. In the event that an employee's Garda vetting raises concerns the information will be dealt with on a confidential basis. All information pertaining to such a situation must be stored in the same way as other data. The Service will not pass on a copy of an employee's Garda Vetting Form to any other party. The Service will hold original Garda Vetting forms.

We will also hold copies of police checks for staff who have lived in other countries (from age 18 years). The staff member holds the original and we hold a certified copy.

Data Erasure and Disposal

When documentation or computer files containing personal data is no longer required, the information must be disposed of carefully to continue to ensure the confidentiality of the data.

For paper-based files and information no longer required, employees should safely dispose of documents or media in shredding receptacles (locked consoles and wheelie bins where there is no access to the documents once deposited). The data will be shredded onsite by the Data Controller

In the case of personal information held electronically, temporary files containing personal information should be reviewed regularly and deleted when no longer required.

When personal data reaches the point where the retention period has expired, the information should also be securely deleted and removed.

In the event that IT equipment containing personal data is no longer required, all data stored on the devices must be removed prior to disposal and the equipment

must be destroyed by a certified supplier who will provide a Certificate of Destruction to conform to the GDPR regulations.

CCTV

The Service does not currently have CCTV. However there is CCTV outside all of our premises. Signs are displayed and staff and parents are notified of their existence.

DATA BREACHES

Definition: A data breach is an incident in which the Service's staff or client's **personal data or that of a child has been lost, accessed, and/or disclosed in an unauthorised fashion.**

This would include, for instance, loss or theft of a laptop, tablet, mobile phone or any other form of communication device containing client or staff details, an email with personal information being sent to the wrong recipient, as well as more organised incidents of external hacking.

Your Responsibility and Immediate Action Required

All employees have a responsibility to take immediate action if there is a data breach.

- If an employee suspects at any time and for any reason that a breach may have occurred, then there is a **need to report it to the Manager/Data Controller as an urgent priority**
- Once notification of an actual or suspected breach has been received, the Manager/Data Controller will put the **Data Breach Procedure** into operation with immediate effect.

DATA SUBJECT RIGHTS/SUBJECT ACCESS REQUEST HANDLING

Privacy Notices

The Service aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used, and
- How to exercise their rights.

For parents of children this is set out in the Service's **Privacy Notice**, provided when they first apply to register their child with the Service.

For new staff members, this is set out as part of the contract and induction material supplied at time of recruitment.

Subject Access Requests

All individuals who are the subject of personal data held by the Service are entitled to:

- Ask **what information** the Service holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the Service is **meeting its data protection obligations**.

If a person the Service requesting this information, this is called a Subject Access Request.

The handling of access requests is described in more detail in the **Subject Access Request ("SAR") Handling Procedure.**

APPENDICES - RELATED DOCUMENTATION

Appendix I: Staff Confidentiality Agreement

Appendix II: Privacy Notice for Staff, Students, and Associates (e.g. Trainers)

Appendix III: Privacy Notice for Parents/Guardians

Appendix IV: Subject Access Request Handling Procedure

Appendix V: Data Breach Handling Procedure

Appendix VI: Website Privacy Notice

Appendix VII: Supplier Documents

Appendix VIII: Personal Data Register: Early Years Services

APPENDIX I: STAFF CONFIDENTIALITY AGREEMENT

Name of Staff Member: _____

Role: _____

I understand and accept that I have a duty of privacy and confidentiality to the Childcare Service and the children, both during and after my period of employment. I undertake:

- To treat all personal information, accessed as part of my role in the service, as private and confidential,
- To only to access children's records where I have a duty of care to the child,
- Not to remove documents or digital records from the Service without the consent of the manager,
- Not to discuss confidential personal information referring to parents, guardians or children with my family or in public, and
- To maintain the privacy of records by ensuring that records are stored securely, and that documents, reports and computer screens are not open to public view.

I understand that a breach of confidentiality is grounds for censure or dismissal.

Name of Staff Member: _____

Signature: _____

Date: __ / __ / ____

APPENDIX II: PRIVACY NOTICE FOR STAFF, STUDENTS AND ASSOCIATES (E.G. TRAINERS)

Your Personal Data: What the Service Needs

EY Service*** is what is known as the 'Controller' of the personal data you provide to us. We take your privacy seriously, and will only use your personal information to process your application for employment and manage your ongoing contract of employment with the Service if you are successful.

The Service collects a range of personal data about staff, applicants for job roles, students, and associates.

This is in order to establish that you are competent and appropriately qualified to work or have work experience in the Early Childhood Care and Education environment. This includes your name, date of birth, address, details of your next of kin, official photo identification, your PPS number, and information necessary for Garda vetting and police check purposes. In addition, **with your consent**, we will collect further medical and health details and other information relevant to the type of work you will be involved in.

Job applicants will provide the above data **except for** Date of Birth, Details of Next of Kin, PPS number official ID, Health Details, and Garda vetting. This information is only sought for successful applicants.

Students and Associates will provide the above data **except for** Date of Birth, PPS number, and Health Details.

Why the Service Needs Data/Purpose of the Processing

We need your personal data to ensure that you are qualified and able to work with and provide safe care and education to children and for us to be able to employ you

in this capacity. The Service will not collect any personal data from you it does not need to provide and oversee your ongoing employment.

What the Service Does with Data/Disclosure

All the personal data is processed by authorised persons (Management or those designated by Management). To run our business and deliver a service, we may need to share your details with:

- Relevant funding bodies such as DCYA, Pobal and the Childcare Committees
- Regulators such as TUSLA, the Revenue Commissioners and the WRC
- Inspectors (TUSLA, Department of Education and Science and Health & Safety Authority)
- External personnel such as payroll and HR contractors, accountants and professional advisors

No other third parties have access to your personal data unless the law allows them to do so.

The Service has a Data Protection regime in place to oversee the effective and secure processing of your personal data.

How Long the Service Keeps Data/Retention Period and Criteria Used

The Service will keep your basic personal data for as long as you remain an employee, and where necessary will continue to hold information on former employees for legal and administrative purposes. More information on the Service's retention procedures can be found by contacting the Manager/Data Controller directly at the addresses given below.

Completed application forms for unsuccessful candidates are disposed of after six months.

What are your rights?

If you wish to see what information we hold on you, simply contact the Manager either by post or and we will endeavour to respond to you within 30 days of receipt of your request.

If at any point you believe the information the service processes on you is incorrect, you may request to have it corrected. You can contact the Manager at the address shown below. If you wish to raise a complaint on how the Service has handled your personal data, you can also contact the Manager.

Data Controller: Ciara Watson and Kara Gargolinski McAlister

If you are not satisfied with our response or believe we are not processing your personal data in accordance with the law, you can complain directly to the Office of the Data Protection Commissioner at:

Email: info@dataprotection.ie
Postal Address: Data Protection Commissioner,
Canal House,
Station Road,
Portarlington
R32 AP23 Co. Laois

Some Key Definitions within GDPR:

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Child Care and EYE Services are controllers of the data

concerning parents, guardians and children that they use to provide Child Care and EYE Services.

Note: if the EYE Service is a legal entity, then the Service itself is the data controller. Otherwise one or all of the principals of the service should be identified as the data controller, or joint data controllers.

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'Data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.

'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

APPENDIX III: PRIVACY NOTICE FOR PARENTS/ GUARDIANS

Your Personal Data: What the Service Needs

EY Service*** is what is known as the 'Controller' of the personal data you provide to it. We take your privacy seriously and will only use personal information about you and your child to provide the services you have requested from us and administer your account.

We collect a variety of personal data to be able to deliver the service requested by you. Most of this data is captured on an enrolment form or on the forms required to obtain government funded fees or fee subsidisation (where applicable).

The enrolment form includes your name, address, details of your child including date of birth plus further detail on any specific medical and other relevant health-care details, and history necessary to allow us to ensure the welfare and safety of your child. Because of the sensitive nature of much this information, you will be asked to confirm your consent for us to collect and hold the information before it does so.

In addition to this, the Service will, at your request and again with your consent, gather additional information on your nationality, religion, and ethnic origin, if you believe this to be an important factor in providing the appropriate care and support for your child.

The enrolment form also collects the contact details and phone numbers of your child's emergency contacts and authorised collectors. You are required to ensure these persons agree to their information being stored and you will be asked to confirm this on the enrolment form.

The Funding Forms may collect personal data including your PPS number and your social welfare status. This is only collected to allow us process funding applications

on your behalf to allow you access subsidies or free care and education for your child (where eligible and applicable).

Why the Service Needs Data/Purpose of the Processing

The Service needs your basic personal data to provide you with its services in line with this overall contract. The Service will not collect any personal data from you it does not need to provide and oversee this service to you.

What the Service Does with Data/Disclosure

All the personal data is processed by management or by staff designated by Management. To deliver our services effectively, we may need to exchange your details with:

- The relevant funding bodies such as DCYA, Pobal, and the Childcare Committees,
- Regulators such as TUSLA or the Revenue Commissioners,
- Inspectors (TUSLA, Department of Education and Science and Health & Safety Authority), or
- External personnel such as HR contractors, accountants and professional advisors.

The Service has a Data Protection Policy in place to oversee the effective and secure processing of your personal data.

How Long the Service Keeps Data/Retention Period and Criteria Used

The Service will keep your and your child's personal data for as long as he or she remains within the Service, and for the period afterwards required by the relevant statutory and legislative guidelines that apply. More information on the Service's retention procedures can be found by contacting the Manager directly at the addresses given below.

What are your rights?

If you wish to see what information the Service holds on you or your child, simply contact the Manager either by post or email and we will endeavour to respond to you within 30 days of receipt of your request.

If at any point you believe the information the Services processes on you is incorrect, you may request to have it corrected. You can contact the Manager at the address shown below. If you wish to raise a complaint on how the Service has handled your personal data, you can also contact the Manager.

Data Controller: Ciara Watson and Kara Gargolinski McAlister

If you are not satisfied with our response or believe the Service is not processing your personal data in accordance with the law, you can complain directly to the Office of the Data Protection Commissioner at:

Email: info@dataprotection.ie
Postal Address: Data Protection Commissioner,
Canal House,
Station Road,
Portarlington
R32 AP23 Co. Laois

APPENDIX IV: SUBJECT ACCESS REQUEST HANDLING PROCEDURE

EY Service*** (the "Service")

Subject Access Request Handling Procedure

What is a Subject Access Request (SAR)?

A SAR is a request for personal information that the Service may hold about an individual. If an individual (or another individual authorised to do so on their behalf) wishes to exercise a subject access right, the request must be made in writing.

Although from time to time an individual may request details of some elements of their personal data held by telephone, formal SARs must be submitted in writing, either electronically or by post.

The purpose of a SAR is to make individuals aware of and allow them to verify the lawfulness of processing of their personal data. Under the GDPR and the current Data Protection Acts (DPA), individuals have the right to obtain confirmation as to whether personal data is being processed. If personal information is being processed, they are entitled to access the following information:

- the reasons why their data is being processed,
- the description of the personal data concerning them,
- anyone who has received or will receive their personal data, and
- details of the origin of their data if it was not collected from them.

SAR Handling - Appointment of a Designated Person

To ensure SARs are responded to in a timely and effective manner, responsibility for identification and management of all requests will be assigned to a Designated Person ("DP"). In the Service the DP is Ciara Watson In the event where the DP is unavailable for any extended period, the organisation will delegate responsibility to a deputy.

Response Time

Under the GDPR, the Service must respond to SARs **within 30 days of receipt.**

This deadline can be extended by a further two months where there are several requests, or the request is complex, but **we must contact the individual within the initial 30 days of receipt**, explaining why the extension is necessary, and when the information will be made available.

Provision of information

Individuals can make a formal SAR electronically/by email or in writing. When a data subject makes the request by email, the response also should be provided in email format unless otherwise requested by the data subject.

In all cases the **individual's identity must be verified** prior to granting access to information. Where insufficient information is provided to verify the identity of the individual and their right to access the personal data, the individual should be contacted in writing, or by phone if appropriate, to request the additional information necessary.

SAR Tracking and Response

1. On receipt of an SAR through any of the above channels, the request must be copied and forwarded to the Designated Person, where it will be recorded on file.
2. Where staff have personal e-mail accounts where a SAR could be made to, these should be monitored when the member of staff is absent to ensure that SARs are dealt with quickly. Remember – we only have up to 30 days to respond, so we need to ensure the relevant information is collated and returned on time.
3. On receipt of the SAR, the Designated Person will log the nature of the SAR request and allocate responsibility for preparation and return of the response. Where the required information cannot be provided within the designated 30

day's timeframe, a letter of explanation must be issued with details of the reason for the delay, and confirmation as to the expected date when the information will be supplied. On issue of the formal response letter, the date of issue will be logged, and a copy of the material sent stored on file for future reference

Right to Withhold Personal Data

Under the GDPR, organisations can withhold personal data if disclosing it would *'adversely affect the rights and freedoms of others.'* This is not likely to the case with the majority of SARs being received, but if in doubt, cross check with the Manager of the Service, or the Data Controller.

Fees

Under the GDPR, a request for personal information is free unless the request is *'manifestly unfounded or excessive'*. In which case the Service can charge a *'reasonable fee'* for multiple requests. This would include both multiple requests, or requests for additional copies of the information.

As with all matters arising with respect to Data Privacy and/or the GDPR, if in doubt with regards to any aspect of a Subject Access Request - refer any questions or concerns to either the Manager or Data Controller.

Sample SAR Response Letter 1 (Put on your headed paper)

Name

Address line1

Address line 2

Town

Date: / /

Subject: Response to your personal information
Subject Access Request (SAR)
Received: [Date] / /

Dear [insert name],

Regarding your recent query, I am pleased to confirm that we hold the following personal information about you and/or your child:

Name:
Date of Registration / Commencement of Service [Date] / /
Date of Termination of Service [Date] / /
Name of Child [Name]
Relationship
DoB [Date] / /

Contact Details:
Address
Telephone
Email number

Other / Additional Information:

[Please describe]

Signed:

Position: Manager on behalf of EY Service***

Sample SAR Response Letter 2: More Information required for verification

(put on headed paper)

Name

Address line1

Address line 2

Town

Date: xx/yy/zzzz

Subject: **EY Service*** (the "Service")**
Response to your personal information
Subject Access Request (SAR)

Received: **mm/nn/pppp**

Dear [Insert Name],

I am writing to you in response to your Subject Access Request.

Regarding your query, to comply with Data Protection law and the Service's own Data privacy rules, it is important for the Service to be able to:

a) Ensure it has sufficient information to be able to verify the identity of the person making the request

b) And in the case where the request is coming from somebody other than the data subject and acting on their behalf, establish that the request is coming from somebody with the appropriate authority to do so.

Accordingly, will you please supply the following information for us to be able to make the necessary verifications before release of the data:

(TBC - on a case by case basis)

Name: AN. Other

Contact Details:

Address

Telephone

Signed:

Position: Senior Manager

/on behalf of EY Service***

APPENDIX V: DATA BREACH HANDLING PROCEDURE

EY Service***

What is a Data Breach?

A data breach is an incident in which personal data held by the organisation on staff, clients or members has been lost, accessed, and/or disclosed in an unauthorised fashion.

This would include, for instance, loss or theft of a laptop, tablet, mobile phone or any other form of communication device containing personal data, an email with personal information being sent to the wrong recipient, loss of paper files or records containing personal data, as well as more organised incidents of external hacking.

The purpose of the Data Breach procedure is to ensure all necessary steps are taken to:

(i) Contain the breach and prevent further loss of data

(ii) Ensure data subjects affected are advised (where necessary)

(iii) Comply with the law on reporting the incident to the Data Protection Commissioner if necessary

(iv) Learn from the incident - identify what measures can and should be put into place to prevent similar occurrences in the future

Data Breach Response Plan - Immediate Action Required

- **Nominate Breach Incident Manager** and designate formal point of contact.
- Identify Stakeholders
- **Set up breach response handling team** - can comprise of the Manager / Support Staff / external IT supplier / partner representatives / third party representatives as deemed necessary

- **Work systematically through six-step process** overleaf, evaluating key steps required and critical outcomes at each stage

Note: Given the strict rules on the management of data breaches, if in doubt about any element of the process, refer any questions or concerns to either the Manager or the Data Protection Officer without delay.

The Need to Inform Data Subjects

"*Data controllers who have experienced an incident giving rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data must give immediate consideration to notifying the affected data subjects. As the Code states, "this permits data subjects to consider the consequences for each of them individually and to take appropriate measures." The consequences may include the potential for fraud / identity theft, but it may also involve the potential for damage to reputation, public humiliation or even threats to physical safety."* (extract from the DPC Guidance on Breach Notification)

The information communicated to data subjects should include information on the nature of the personal data breach and a contact point where more information can be obtained. It should recommend measures to mitigate the possible adverse effects of the personal data breach.

The Need to Inform the Office of the Data Protection Commissioner (DPC)

" .. the Code of Practice states that ***all incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner.*** *The only exceptions are when the data subjects have already been informed* ***and*** *the loss affects no more than 100 data subjects* ***and*** *the loss involves only non-sensitive, non-financial personal data. The Code also makes clear that if a doubt exists - especially whether the technological measures protecting the data are such as to permit a reasonable conclusion that the personal data has not been put at risk - the matter should be reported to the Office of the Data Protection Commissioner."* (extract from the DPC Guidance on Breach Notification)

Complex personal data security breach incidents may take a considerable period to fully investigate and resolve. **The initial contact with the Office should be limited to describing the facts as they are known and the steps being taken to address those facts**. The personal data involved should **not** be included in such reports to the Office of the Data Protection Commissioner.

Responsibility for Communication of Breach

In the event of a data breach, it is the responsibility of the Designated Person or Manager (see below) to determine which notifications are necessary and to ensure they take place without delay. The **maximum timeframe for notification** to the Office of the Data Protection Commissioner has been set at **72 hours** from the time the incident is first discovered.

Data Breach - Six Step Process

1. **Identification and Confirmation:** Identify and confirm volumes and types of data affected, and all data subjects/members involved.
2. **Containment - typically:**

a. Identify source of breach

b. Limit scope of negative impact

c. Isolate - database/network/mobile devices

d. Denial of login access

e. Partial or complete systems lockdown

3. **Analysis**: Detailed analysis of volumes and types of data involved & identify gateways/source/location and cause of data loss.
4. **Notification of DPC / Data Subjects / Other:** Timing is critical. Consider need to inform:

a. Data subjects, whether notification is urgent and/or necessary need for further action on their part (change passwords, notify banks/ etc)

b. Supervisory Authority i.e. Office of the DPC (within 72 hours of first becoming aware of the breach)

c. Other third-party stakeholders

5. **Damage Control**: In the event of major breach:

a. Advise and involve highest level of management / partner / public body representatives.

b. Have a communication plan in place for Data Subjects, Regulators, Public Bodies, Press, etc.

c. Channel all communication through a single source e.g. coordinated press-releases.

d. Review all third-party contracts - be aware of your responsibilities and liabilities.

6. **Lessons Learned**

a. Conduct thorough lessons learned exercise.

b. Improve processes to avoid future data breaches.

c. Consider independent/third-party audit to review your organisation's policies and compliance efforts, as well as its technical infrastructure.

Further Information:

For more information in this key area, please see the following guidelines issued by the Office of the Irish Data Protection Commissioner:

Personal Data Security Breach Code of Practice

https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

Breach Notification Guidance

https://www.dataprotection.ie/docs/Breach_Notification_Guidance/901.htm

APPENDIX VI: WEBSITE PRIVACY NOTICE

How we use your information:

This privacy notice provides information about the ways in which EY Service*** collects, stores, shares or keeps personal information provided by our customers. We will only use information you provide in order to make contact with you to supply the information on our services, or regarding jobs or employment with EY Service*** that you have requested.

Using our website:

Our website uses cookies. The purpose of the cookies is solely to assist us in managing our website.

Emailing us:

Any emails sent to us and any messages received through our online contact form are recorded and forwarded to the relevant section. The sender's email address will remain visible to all staff tasked with dealing with the query.

Data Protection Commissioner; Dublin and Portarlington

+353 61 104 800 | email info@dataprotection.ie

APPENDIX VII: SUPPLIER DOCUMENTS

(TEMPLATE LETTER TO SUPPLIER)

Dear _____,

I am writing to you as a supplier who handles data relating to our Service. This is to ensure compliance with the General Data Protection Regulations and is part of the Service's due diligence process.

Under Article 28 (1) of the GDPR we can only use a supplier (data processor) who is “providing sufficient guarantees to implement appropriate technical or organisation measures, in such a manner that processing will meet the requirements of this regulation”

We have developed a short due diligence questionnaire which we are asking you to complete.

The following applies to our Service in relation to data protection:

1. Personal data must be fairly and lawfully processed
2. Accuracy- personal data must be accurate and kept up to date
3. Security- personal data should be kept secure in terms of encryption and accessibility
4. Keep data no longer than is necessary
5. Individual rights- right of access to information, right of rectification
6. Information is only shared with those who need it

Please return the questionnaire as soon as possible.

Yours sincerely,

Manager

Processor Due Diligence Questionnaire

Please complete and email to: Email address

Name of Early Years' Service: EY Service***

Name of Supplier (insert name of supplier)

Requirement	YES / NO	Comment:
Do you have a knowledge and understanding of the GDPR legislation and your responsibilities as data processor? Use the		
Do you have a Data Protection Policy? Please attach on return		
Do you use subcontractors and if so have you ensured they are GDPR compliant? Use the comments box		
Is the data held on a secure server? Use the comments box to give		
Do you and any subcontractors have a documented procedure for deleting subject records on request (including archived/back-up		
Do you agree that all records will be deleted on terminating of contract with your company at no extra cost?		
Do you have the required privacy notices which meet GDPR requirements?		

Do your contracts of employment and disciplinary procedures list confidentiality and breach of data privacy as gross misconduct?		
Is any IT equipment that hold personal data encrypted by you and any subcontractors? Please use comments box to give details of		

I agree that the above is a true and accurate reflection of our GDPR compliance.

Signed: _____

Date: _____

Personal Data Register: Purpose and Lawfulness of Processing

The following table shows the categories of personal data processed by the Service, the Purposes for processing, and the lawful basis under which the data is processed.

Category of Personal Data	Purpose of Processing	Lawfulness of Processing
The Child		
Child's Name, Address and Date of Birth. Child's PPS number on welfare letter. Child's Birth Cert	Necessary to support the administration of the Early Years Service	Article 6.1(b) in relation to entering into a contract and getting paid for providing a service to children and parents Article 6.1(c) Processing is necessary for compliance with a legal obligation to which the controller is subject (Revenue and Legal obligations)
Child's Medical History (conditions and allergies), Information on child's disability, Child's Vaccination Record, Medicines used by child, Medical Emergencies, Accident and Incidents,	Necessary to provide the Child Care Service and safeguard the Health and Wellbeing of the child	**Special Categories of Personal Data** Article 6.1(b) in relation to entering into a contract and getting paid for providing a service to children and parents Article 6.1(c) Processing is necessary for compliance with a legal obligation to which the controller is subject including Revenue and Legal obligations **(ref: The Childcare Act 1991 (Early Years Services)**
Care Orders/ Custody Information, Child Protection Reports, Police Reports	Necessary to provide the Child Care Service and safeguard the Health and Wellbeing of the child	Article 6.1(c) Processing is necessary for compliance with a legal obligation to which the controller is subject **(ref: Children First Act 2015**)
Aistear (Learning) Assessments/ Observation Developmental Observation Record	Necessary to support the administration of the The Early Years Service	Article 6.1(b) in relation to entering into a contract and getting paid for providing a service to children and parents

Photographs (individual and with other children), Video, CCTV images (if applicable)	Necessary to provide the Early Years Service and safeguard the Health and Wellbeing of the child	Article 6.1(a) The Parent or Guardian of the Child has given **Consent** to processing of his or her personal data for one or more specific purposes
Nationality, religion and ethnic origin	Collected only if explicitly requested by parents to ensure provision of a suitable and appropriate environment for the development of the child in accordance with the parent's wishes	Article 6.1(a) The Parent or Guardian of the Child has given **Consent** to processing of his or her personal data for one or more specific purposes

Category and Personal Data held	Purpose of Processing	Lawfulness of Processing
Parents and Guardians		
Parent/Guardians Names, Addresses, Contact Details, place of work. Contact details for child's emergency contacts. Contact details for child's authorised collectors Parent Date of Birth Parent PPS number Letter from social welfare stating type of welfare payments. Letter stating employment details if on	Necessary to support the administration of the Childcare Service and safeguard the Health and Wellbeing of the Child	Article 6.1(b) Processing is necessary in relation to entering into a contract and getting paid for providing a service to children and parents and Article 6.1(c) Processing is necessary for compliance with a legal obligation to which the controller is subject (Revenue and Legal Obligations Ref; Childcare Act 1991 (Early Years Services Regulations 2016)

Category and Personal Data	Purpose of Processing	Lawfulness of Processing
Staff and Job Applicants Plus, **Trainers, Associates, Students. Volunteers**		
CV and/or application form, Address and Contact details, Next of Kin, Pay Slips / PPS number, Official ID, Meetings and Internal Training Documents, HR documents (disciplines, grievances etc) Copies of Qualifications and Training Certs, Validated references, Garda Vetting, Police Checks	Necessary to support the administration of the Childcare Service and Contract of Employment and safeguard the Health and Wellbeing of the child	Article 6.1(b) Processing is necessary in relation to entering into a contract of employment with the Childcare Service Article 6.1(c) Processing is necessary for compliance with a legal obligation to which the controller is subject (Revenue and Legal obligations: Ref: Childcare Act 1991 (Early Years services) Regulations 2016)
Medical History (including vaccinations), Medical Reports, Medical Certs	Necessary to support the administration of the early Years' Service and Contract of Employment and safeguard the Health and Wellbeing of the child	**Special Categories of Personal Data** Article 6.1(a) The Data Subject has given **Consent** to processing of his or her personal data for one or more specific purposes Consent

Personal Data Register: Early Years Services

This Register describes the personal data held by EY Service***

Data Controller: Ciara Watson and Kara Gargolinski McAlister

Purpose of Processing

The personal data collected is used for the provision of Childcare services to the parents and guardians of the children and to ensure a safe working environment for the protection of both staff and children. The data has been collected to fulfil the Service's contractual obligations to deliver the service. Where there is a requirement to collect and process data falling into the Special Category or sensitive data as described under GDPR, the necessary consent is obtained from parents/guardians and staff at the outset. The personal data is only used for the purposes described.

APPENDIX VIII Personal Data Register: Early Years Services

Category of Data Subject: CHILD						
	Type of Data	**Storage of Data**	**Who has access to data**	**Information Security- Technical and**	**Retention Period/ Timeline for Disposal**	**How is data disposed**
1.	Child's Name, Address and Date of Birth	This data is stored on the Child Registration Form (manual or electronic), Medicine Records and Accident/ Incident Records. It is also input into the PIP system for funding purposes. Attendance Books Check in/ Check Out register	**Internally** Staff and Management **Externally** Software Supplier Regulator Tusla Funders and Funding Agencies: DCYA, Pobal and Childcare Committee Professional advisors (e.g. Legal)	Registration Forms are held under lock and key Other records are only accessible to staff in the rooms who are vigilant that the records are not accessible or on display Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communicatio n device are password	2 years for TUSLA (from time the child ceases in the Service) Information may be required to be held longer than 2 years (e.g. where there has been an accident that required medical intervention or where a child was injured or child protection information) [These are examples only please ensure that you have an objective reason for	Shredded internally or externally Electronic data destructed
1.	Child's Name,					

2.	Child's Medical History (conditions and allergies)	This data is stored on the Child Registration Form (manual or electronic), Medicine Records, Care Plans Therapists/ Advisors/ Mentor's reports It may also input into the PIP system for funding purposes.	**Internally** Staff and Management **Externally** Software Supplier Regulator Tusla Funders and Funding Agencies: DCYA, AIM, Pobal and Childcare Committee Professional advisors (e.g. Legal) Other professional such as psychologists and other therapists	Registration Forms are held under lock and key Other records are only accessible to staff in the rooms who are vigilant that the records are not accessible or on display Electronic data is held on a secure server Electronic information is encrypted, and PCs/Laptops, tablet, mobile phone or any other form of communication device are password protected Privacy Statement is	2 years for TUSLA (from time the child ceases in the Service)	Shredded internally or externally Electronic data destructed

3.	Information on child's disability (additional need)	This data is stored on the Child Registration Form (manual or electronic), Medicine Records, Care Plans Therapists/ Advisors/ Mentor's reports It may also input into the PIP system for funding purposes.	**Internally** Staff and Management **Externally** Software Supplier Regulator Tusla Funders and Funding Agencies: DCYA, AIM, Pobal and Childcare Committee Professional advisors (e.g. Legal) Other professional such as psychologists and other therapists	Registration Forms are held under lock and key Other records are only accessible to staff in the rooms who are vigilant that the records are not accessible or on display Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are	2 years for TUSLA (from time the child ceases in the Service)	

4.	Child's Vaccination Record	Child Registration Form Electronic Record Email	**Internally** Staff and Management **Externally** Software Supplier Regulator Tusla	Registration Forms are held under lock and key Other records are only accessible to staff in the rooms who are vigilant that the records are not accessible or on display Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password protected Pri...	2 years for TUSLA (from time the child ceases in the Service)	

5.	Child Protection Reports (if relevant)	Child's file Electronic Record Email	**Internally** Staff and Management (on a "need to know" basis, not all staff) **Externally** Regulator Tusla Professional advisors (e.g. Legal or HR including HR investigators) Gardaí Other professionals as relevant	Reports kept under lock and key Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password protected Privacy Statement in place	2 years for TUSLA [from the date the child ceases in the Service] or as advised by Insurance or Other Professionals if case pending.	

6. 6.	Medicines used by child Medicines used by child (contd.)	Medicine Record Care Plans Medicine labels Apps	**Internally** Staff and Management **Externally** Software Supplier Regulator Tusla Professional advisors (e.g. Legal) Other professionals such as medical personnel	Medicine forms kept discreetly in rooms and only accessible to staff Staff are vigilant that the records are not accessible or on display Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communicatio n device are password	2 years for TUSLA (from time the child ceases in the Service)	

7. 7.	Accident and Incidents Accident and Incidents (contd)	Accidents & Incident Book /Form Software Apps	**Internally** Staff and Management **Externally** Software Supplier Regulator Tusla Professional advisors (e.g. Legal) External Investigators HAS Insurance Company Other professionals such as medical personnel	Accident forms kept discreetly in rooms and only accessible to staff Staff are vigilant that the records are not accessible or on display Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of	2 years for TUSLA (recommended up to the age of 21 for insurance purposes)	
8. 8.	Medical Emergencies Medical Emergencies	Report on Medical Emergency Medical Emergency Plan Apps	**Internally** Staff and Management **Externally** Software Supplier Regulator Tusla Professional advisors (e.g. Legal) External Investigators HAS Insurance Company Other professionals such as medical personnel	Emergency Plans kept discreetly in rooms and only accessible to staff Staff are vigilant that the records are not accessible or on display Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of	2 years for TUSLA (recommended up to the age of 21 for insurance purposes)	

9.	Photographs (individual and with other children)	Learning Journals Wall Displays Newsletters Facebook Website Learning Journals Software App	**Internally** Staff and Management **Externally** Software Supplier Parents and visitors Regulator Tusla DES Professional advisors (e.g. Legal) Other parents	Permissions are sought for the taking of photographs and for sharing photos (website, Facebook, newsletters etc) Permission is sought from all parents in respect of group photographs A policy is in place for Internet, Photographic and Recording Devices Electronic data is held on a secure server Electronic information is encrypted, and PCs/	Displays and portfolios of photos will be kept for 2 years. Learning stories will be sent home annually with children and copies will not be kept Images on the website or Facebook will be kept for 2 years	Images will be deleted immediately from phones and saved on a more secure device Images will be deleted from websites and Facebook and electronic devices after 2 years unless further permission is granted
9.	Photographs (individual					

10.	Video	Website Facebook Open Facebook Closed Software app (WhatsApp	**Internally** Staff and Management **Externally** Software Supplier Parents and visitors Regulator Tusla DES Professional advisors (e.g. Legal) Other parents	Permissions are sought for the taking of video and for sharing photos (website, Facebook, etc.) Permission is sought from all parents in respect of group videos and parents can opt out A policy is in place for Internet, Photographic and Recording Devices Electronic data is held on a secure server Electronic	Recordings are kept for 1 month	
11. 11.	CCTV images (if applicable) CCTV images (if applicable) contd.	CCTV storage tapes	**Internally** Staff and Management **Externally** CCTV supplier Technical expert if images must be redacted Data subject when there is a SAR Regulator	CCTV Policy in place Signage in place CCTV not used for daily monitoring	28 days (unless under investigation or an issue)	

12. 12.	Care Orders/ Custody Information Care Orders/	Child File Email	**Internally** Staff and Management on a need to know basis only **Externally** Regulator Tusla Gardaí Insurance Company Professional advisors (e.g. Legal) Legal Advisors Other professional advisors	Information is held under lock and key Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password protected Privacy Statement in place Due diligence	2 years for TUSLA (from time the child ceases in the Service)	
13. 13.	Child's PPS number on welfare letter Child's PPS number on welfare letter (contd)	PIP Portal	**Internally** Staff and Management (whoever administers PIP) **Externally** Pobal (PIP)	PPS numbers are held under lock and key until submitted Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password protected Privacy Statement in place Due diligence questionnaire	Only for the length of time it takes to submit child on to the PIP system and generate a DCYA number	

14.	Child's Birth Cert	Child's file	Management only Administrator of PIP	Birth Certificates are held on the Child's File. These	Birth Certificates are only held until such time as the	Shredded
15. 15.	Developmental Observation Record Developmental Observation Record (contd)	Child File in paper form Software app	**Internally** Staff and Management **Externally** Regulator Tusla Professionals such as therapists with permission Professional advisors Mentors Software supplier Primary School with permission	Developmental Observations are held under lock and key under the child's private file Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password protected Privacy Statement in place Due diligence questionnaire	Send home with family when child finishes unless you have a specific reason for keeping	

16. 16.	Aistear (Learning) Assessments / Observation Aistear (Learning) Assessments /	Scrapbooks Learning Journals Software app (Little Vista, Child Diary, Eccesoft)	**Internally** Staff and Management **Externally** Regulator Tusla Professionals such as therapists with permission Professional advisors Mentors Department of Education and Science(DES) Software supplier Primary School with permission	Aistear Assessments are held in the class/care room discreetly Electronic data is held on a secure server Electronic information is encrypted and PCs/Laptops, tablet, mobile phone or any other form of communication device are password protected Privacy Statement in	Send home with family when child finishes unless you have a specific reason for keeping	
Category of Data Subject: PARENTS/GUARDIANS, Authorised Collectors,						

17.	Parent/ Guardians Names, Addresses, Contact Details, place of work	Child Registration Form In Roll Book (Attendance Book) or separate Record in Care Rooms or brought on outings	**Internally** Staff and Management **Externally** Regulator Tusla Professional Advisors	Registration Forms are held under lock and key Other records are only accessible to staff in the rooms who are vigilant that the records are not accessible or on display Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password protected Privacy	2 years for TUSLA (from time the child ceases in the Service)	
17.	Parent/ Guardians Names, Addresse					

18.	Parent Date of Birth Parent PPS number, Letter from social welfare stating type of welfare payments . Letter stating employment details if on employment scheme	These documents are scanned and stored on PIP system	**Internally** Staff and Management **Externally** DCYA Pobal Professional Advisors	Information held under lock and key until submitted Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password protected Privacy Statement in place	Submission timeframe for funding scheme only	
Category of Data Subject: STAFF						

19.	CV and/or application form	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Tusla Legal/HR and other Professional Advisors Insurance Company Regulatory authorities such as Revenue, WRC or HSA Inspectors	Staff files are held under lock and key Staff telephone numbers are not on display or accessible Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device	1 year for candidates not selected. 6 years after staff member leaves employment.	
20.	Address and Contact details	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Tusla Legal/HR and other Professional Advisors Insurance Company Regulatory authorities such as Revenue, WRC or HSA Inspectors	Staff files are held under lock and key Staff telephone numbers are not on display or accessible Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communicati	6 years after a staff member leaves employment.	
20.	Address and Contact Details (contd.)					

21.	Copies of Qualifications and Training Certificates	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Tusla Legal/HR and other Professional Advisors Insurance Company Regulatory authorities such as Revenue, WRC or HSA Inspectors	Staff files are held under lock and key Staff telephone numbers are not on display or accessible Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password protected Privacy Statement in place	6 years after a staff member leaves employment.	
21.	Copies of Qualifications and Training Certificates					

22. 22	Validated references Validated references (contd)	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Tusla Legal/HR and other Professional Advisors Insurance Company Regulatory authorities such as Revenue, WRC or HSA Inspectors	Staff files are held under lock and key Staff telephone numbers are not on display or accessible Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are	5 years from commencement of employment. 1 year after staff leave.	
23. .	Pay Slips/ PPS number	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Legal/HR and other Professional Advisors Insurance Company Regulatory authorities such as Revenue, WRC Inspectors Accounts/ Payroll	Staff files are held under lock and key Staff telephone numbers are not on display or accessible Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device	6 years after staff member leaves employment.	

24.	Official ID	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Tusla Legal/HR and other Professional Advisors Insurance Company Regulatory authorities	Staff files are held under lock and key Staff telephone numbers are not on display or accessible Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are	6 years after a staff member leaves employment.	

25.	Garda Vetting	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Tusla Legal/HR and other Professional Advisors Insurance Company Regulatory authorities	Staff files are held under lock and key Staff telephone numbers are not on display or accessible Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password protected	5 years from commencement of employment.	
25.	Garda Vetting (contd)					
26.	Next of Kin	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Tusla Legal/HR and other Professional Advisors Insurance Company Regulatory authorities	Staff files are held under lock and key Staff telephone numbers are not on display or accessible Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are	6 years after a staff member leaves employment.	
26.	Next of Kin (contd.)					

27.	Meetings and Internal Training Documents	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Tusla Legal/HR and other Professional Advisors Insurance Company Regulatory authorities Inspectors	Staff files are held under lock and key Staff telephone numbers are not on display or accessible Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communicatio n device are	6 years after a staff member leaves employme nt.	
28.	Medical History (including vaccinations)	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Legal/HR and other Professional Advisors Insurance Company	Consent given Staff files are held under lock and key Staff telephone numbers are not on display or accessible Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of	6 years after a staff member leaves employme nt.	

29. 29.	Medical Reports Medical Reports (contd.)	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Tusla Legal/HR and other Professional Advisors Insurance Company Regulatory authorities such	Consent given Staff files are held under lock and key Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password	6 years after a staff member leaves employment.	
30.	Medical Certificates	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Legal/HR and other Professional Advisors Insurance Company	Consent given Staff files are held under lock and key Electronic data is held on a secure server, Electronic information is encrypted, and PCs or Laptops, tablet, mobile phone or any other form of communication device are password protected	6 years after staff member leaves employment.	

31.	HR documents (disciplines, grievances etc.)	Staff file (manual or electronic)	**Internally** Management or persons designated by management **Externally** HR Advisors Software Company Legal/HR and other Professional Advisors Insurance Company Regulatory authorities such as Revenue, WRC or HSA Inspectors	Staff files are held under lock and key Electronic data is held on a secure server Electronic information is encrypted and PCs/ Laptops, tablet, mobile phone or any other form of communication device	6 years after a staff member leaves employment. As advised by Insurance /Legal if required.	
OTHERS						
32.	CVs for trainers / Associates / Students / Volunteers	Paper and/ or Electronic file	Management Tusla	Information held under lock and key until submitted Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are	1 year following termination of any agreement	
32.	CVs for trainers / Associates / Students / Volunteers					

33.	ID for trainers / Associates / suppliers	Paper and or Electronic file	Management Tusla	Information held under lock and key until submitted Electronic data is held on a secure server Electronic Information is password protected and PCSs/ Laptops, tablet, mobile phone or any other form of communicatio n device are	1 year following terminati on of any agreeme nt	
34. 34.	Garda Vetting for trainers / Associates / suppliers / Students / Volunteers Garda Vetting for trainers / Associates / suppliers / Students / Volunteers (contd.)	Paper and/or Electronic file	Management Tusla	Information held under lock and key until submitted Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communicatio n device are password	5 years following commenc ement of engagem ent. 1 year following terminati on of any engagem ent	

35. 35.	References for trainers / Associates / suppliers / Students / Volunteers where applicable References for trainers /	Paper and/or Electronic file	Management Tusla	Information held under lock and key until submitted Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password protected	5 years following commencement of engagement. 1 year following termination of any engagement	
36.	CVs for job applicants (not staff)	Paper and/or Electronic file	Management	Information held under lock and key until submitted Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are	Timeframe of panel if part of recruitment. 1 year recommended if no panel timeframe specified	

37 37. .	Contact details for child's emergency contacts Contact details for child's emergency contacts (contd)	Child Registration Form Software Apps (Little Vista, Child Diary, Eccesoft)	Management Key Workers in Rooms Software Company Tusla	Information held under lock and key until submitted Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password protected Privacy Statement in place Due diligence	2 years for TUSLA (from time the child ceases in the Service)	

38. 38.	Contact details for child's authorised collectors Contact details for child's authorised collectors	Child Registration Form Software Apps (Little Vista, Child Diary, Ecopoet)	Management Key Workers in rooms Software Company Tusla	Information held under lock and key until submitted Electronic data is held on a secure server Electronic information is encrypted, and PCs/ Laptops, tablet, mobile phone or any other form of communication device are password protected Privacy Statement in place Due diligence	2 years for TUSLA (from time the child ceases in the Service)	
Category of Data Subject: Miscellaneous						
39.	Visitors	Visitor's Sign In Book	Management Tusla Garda Síochána Legal / HR	Visitor's Sign In book is held under lock and key for	1 year from the date to which it relates	

Disclaimer

Data and information is provided for informational purposes for the Early Years Section only, and is not intended for any other commercial or non-commercial purposes. Neither us nor any of our data or content providers shall be liable for any errors or delays in the content, or for any actions taken in reliance thereon and service providers should seek legal advice in relation to any specific queries regarding the application of the GDPR to the operation of their service where required.