LINKS CHILDCARE POLICIES & PROCEDURES		
GDPR POLICY		
Last Review Date: June 2023	Policy No.47	Issued: 2018

INTRODUCTION

Why This Policy Exists

Links Childcare 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 parents 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.

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, Links Childcare 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 and 2003 (the "Data Protection Acts") and the 2016 General Data Protection Regulation ("GDPR") describe how organisations including Links Childcare 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 Links Childcare are described below.

The Principles - Management of Personal Data

All personal data collected and held by Links Childcare 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 Links Childcare **Privacy Notice.**

- **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 Links Childcare **Register of Personal Data Records.**

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

Links Childcare 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 Links Childcare 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 Links Childcare 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 families - 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 families 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.

- **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 Parents' Bank Account details

and any and all other information relating to individuals.

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
- Data concerning a person's sex life or sexual orientation.

For this category of Data, should it arise, we will ask your consent at the time an employee

first joins Links Childcare or when a parent/guardian or parents/guardians register their child using the appropriate application or registration forms.

Records of consent will be retained securely for the recommended legal/regulatory periods.

RESPONSIBILITIES AND COMPLIANCE

Policy Scope

Everyone who works for or with Links Childcare has responsibility for ensuring data is collected, stored, and handled appropriately. Each person who 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:
Data Protection Officer: Triona Barrett (Director of Support Service)
Data Controller: Deirdre Kelly (Managing Director)
Child Protection Designated Liaison Person: Pat O' Riordan

- 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 Links Childcare parent website, parent handbook and Employee Handbook.
- There are regular updates to data protection awareness, so that data protection is a "living" process aligned to the way Links Childcare 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 Links Childcare'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

To ensure the implementation of this policy, Links Childcare 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 Links Childcare
- 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.
- ensuring that 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, Links Childcare may invoke the disciplinary policy and procedure in relation to employees. Sanctions include warnings up to and including dismissal for breaching the rules and guidelines 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

Links Childcare will undertake regular reviews of the internal operation and changes in the legislation to ensure ongoing compliance with Data Protection Regulation.

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).
- Links Childcare 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 the HR Department 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 Links Childcare 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 will 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.

When data is **stored on paper,** it will 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 Links Childcare'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.**
- 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 Links Childcare 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 L Links Childcare'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 Links Childcare will disclose requested data; however, the Data Controller must ensure the request is legitimate, seeking assistance from Management and from the Links Childcare's legal advisers where necessary.

Please note that information may need to be disclosed to authorised third parties. Links Childcare 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 PIP System & Pobal Compliance Officers
- Department of Children & Youth Affairs (DCYA)
- Insurance Company
- Health and Safety Authority
- Workplace Relations Commission
- Revenue Commissioners
- HR Advisors
- Other Professional Advisors
- Childcare management software
- Payroll software
- Early Childhood Ireland
- National Employment Rights Authority

Note: Data Collected Through Garda Vetting

Links Childcare 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 will be stored in the same way as other data. Links Childcare will not pass on a copy of an employee's Garda Vetting Form to any other party. Links Childcare will hold original Garda Vetting forms.

Links Childcare 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 Links Childcare holds a certified copy.

Data Erasure and Disposal

When documentation or computer files containing personal data are no longer required, the information will 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 - or alternatively a third party data destruction specialist and vetted staff will collect documents and media and shred off-site. 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 will 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/or the equipment must be destroyed by a certified supplier who will provide a Certificate of Destruction to conform to the GDPR regulations)

CCTV

Links Childcare is a Data Controller as defined under the General Data Protection Regulation (GDPR) and is responsible for the data/information collected using CCTV.

Usage of CCTV is in line with the principles set out in **The Data Protection Acts of 1988 and 2003,** and the **2016 General Data Protection Regulation (GDPR):** Where CCTV contains footage of images which can be clearly identified as a recognisable person, it is deemed to be Personal Data and is covered by the Data Protection Acts and Regulation. In short, where a data controller uses a CCTV it is obliged to comply with all associated data protection obligations.

Purpose of the CCTV

The system has been installed by Links Childcare with the primary purpose of ensuring the safety of children in our care, and helping to ensure the safety of all staff, parents/guardians and visitors, consistent with respect for the individuals' privacy.

This will be achieved by monitoring the system to:

- Ensure that children are appropriately cared for
- Assist in the prevention and detection of crime
- Provide opportunities for staff training
- Investigate accidents.

The system will **not** be used:

- To provide recorded images for the Interne
- To provide images for a third party other than An Garda Síochána, Tusla, or the Child and Family Agency during their enquiries
- For continuous monitoring of staff
- For monitoring staff performance
- As a supervision tool

Note: If after viewing the CCTV for any of the reasons stated above, incidents of inappropriate practice or breach of policies are observed, these can be brought to the attention of the

employee. The employees should be given the opportunity to view the footage. Depending on the circumstances, this may result in the discipline policy and procedure being invoked.

Fairness

Links Childcare and its management respect and support the individual's entitlement to go about his/her lawful business, and this is the primary consideration in the operation of CCTV.

Although there will be inevitably some loss of privacy with CCTV, cameras are not used to monitor the progress or activities in the ordinary course of lawful business. They are used to address concerns, deal with complaints, or support investigations. New employees will be informed immediately at induction that a surveillance system is in operation.
Parents/guardians will be informed when they enrol their child. They will be informed of the purpose of the CCTV and what it can and cannot be used to monitor.

Responsibilities of Management

Management is responsible for the operation of the system and for ensuring compliance with this policy. In particular:

- To ensure the system is always operational
- To ensure that servicing and repairs are carried out as necessary to the system
- To respond to any individual's written request to view a recording that exists of him/her or his/her children
- To ensure prominent signage is in place that will make individuals aware that they are entering a CCTV area.
- To ensure that areas of privacy (toilets etc.) are not monitored using CCTV
- To ensure confidentiality is maintained at all times.

Recorded information will be stored in the office and will only be available to those directly connected with achieving the objectives of the system.

Location of Cameras

The choice of sites for locations of CCTV Cameras will be in line with the primary purposes outlined above, i.e. where they assist in ensuring the safety of children and the safety of all staff, parents/guardians and visitors. Cameras will not be in areas where people expect to have a reasonable expectation of privacy.

The following areas are currently monitored by CCTV in some/all of the following areas:

- entrances
- exits
- corridors
- general assembly areas
- rooms

Signage

Signage should be clearly displayed advising that CCTV is in operation for ensuring the safety of children in our care, and helping to ensure the safety of all staff, parents/guardians and visitors. Notification of CCTV usage can usually be achieved by placing easily-read and well-lit signs in prominent positions. A sign at all entrances will normally suffice.

Right to View or Access Recordings

In line with the requirements of the GDPR, data subjects have the right to request access to their images or personal data captured by CCTV. Management will respond to a request to view a recording by allowing the viewing to take place in the presence of management on the premises. This is to protect other children/staff who may be visible on the recording.

Sharing or Copying Recordings with Data Subjects (i.e. parents, guardians, or staff)

Any person whose image is recorded on a CCTV system also has a right to seek and be supplied with a copy of their own personal data from the footage. To exercise that right, a person must make an application in writing or by email. Links Childcare will not charge for responding to such a request and will respond within 30 days.

In the first instance, the individual should be asked whether they would be satisfied with merely viewing the images recorded.

Recordings will however be provided, where formally requested by parents, guardians, or staff.

- Requests for access to recordings must be made in writing, or by email.
- Sufficient information must be provided to locate the relevant recording, a specific date, and reasonable time window.
- Viewings will take place, if appropriate, in the service in the presence of management.
- Management will have 30 days to respond.
- If a copy of recording is given to a third party, that third party must sign a declaration form that they will not share the tape with anyone else, copy it, or use it for unauthorised purposes.
- An incident report will be completed for each incident requiring investigation.

If access to or disclosure of the images is allowed, then the following should be documented:

- The date and time at which access was allowed or the date on which disclosure was made,
- The identification of any third party who was allowed access or to whom disclosure was made,
- The reason for allowing access or disclosure,
- The extent of the information to which access was allowed or which was disclosed, and
- The identity of the person authorising such access.

Where images of parties other than the requesting data subject appear on the CCTV footage, Links Childcare will arrange to pixelate or otherwise redact or darken out the images of those other parties before supplying a copy of the footage or stills from the footage to the requestor.

If the system does not have the facilities to carry out that type of editing, an editing company may need to be hired to carry it out. If an editing company is hired, then the Manager or

designated member of staff needs to ensure that there is a contractual relationship between the Data Controller and the editing company.

Sharing of CCTV Images with Garda Siochana or other Authorised Third Parties

At times it may be necessary at times to provide copies of recordings to An Gharda Siochana or other authorised parties.

CCTV footage should only be provided to An Gharda Siochana when a formal written request is provided to the data controller stating that Garda Siochana is investigating a criminal matter.

For practical purposes, and to expedite a request speedily in urgent situations, a verbal request may be sufficient to allow for the release of the footage sought. **Any such verbal request must be followed up with a formal written request.** It is recommended that a log of all Garda Síochána requests is maintained by data controllers and processors.

There is a distinction between a request by Garda Síochána to view CCTV footage and to download copies of CCTV footage. In general, Garda Síochána making a request to simply view footage on the premises of a data controller or processor would not raise any specific concerns from a data protection perspective.

For authorised third parties, similar rules apply - copies of CCTV footage can be viewed or made available subject to the requirements and restrictions as set out above**.**

Storage and Retention of CCTV Footage

The storage medium should be stored in a secure environment with a log of access kept. Access should be restricted to authorised personnel.

Traceability

Recordings must be logged and traceable throughout their life in the system. They must be identified by a unique serial number indelibly marked on the media shell.

Time and Date Stamping

The correct time and date must be overlaid on the recording image.

Retention Period

Recordings will be retained for no longer than 48 hours (or as defined in the Links Childcare Personal Data Register - unless there is requirement to retain CCTV footage to assist with the investigation of incidents, accidents, or other serious issues.

DATA BREACHES

Definition: A data breach is an incident in which Links Childcare staff or family personal data has been lost, accessed, and/or disclosed in an unauthorised fashion.

This would include, for instance, loss or theft of a laptop containing child 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 Data Controller as an urgent priority**
- Once notification of an actual or suspected breach has been received, the Data Controller will put the **Data Breach Procedure** into operation with immediate effect.

  Please refer to the **Links Childcare Data Breach Policy.**

DATA SUBJECT RIGHTS/SUBJECT ACCESS REQUEST HANDLING

Privacy Notices

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

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

For parents of children this is set out in the Links Childcare **Privacy Notice**, provided when they first apply to register their child with the Service. A version of this statement is also available on the Links Childcare website.

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 Links Childcare 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 Links Childcare is meeting its data protection obligations.

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

Appendix I: SUPPLIER DOCUMENTS

To whom it concerns

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 Links Childcare 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. Data must be retained 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 faithfully

Processor Due Diligence Questionnaire

Please complete and email to (insert email address)

Links Childcare

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 comment box to demonstrate this		
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 to explain		
Is the data held on a secure server? Use the comments box to give details		
Do you and any subcontractors have a documented procedure for deleting subject records on request (including archived/back-up records?		
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?		

Please attach on return		
Do your contracts of employment and disciplinary procedures list confidentiality and breach of data privacy as gross misconduct? Please attach relevant clauses		
Is any IT equipment that hold personal data encrypted by you and any subcontractors? Please use comments box to give details of encryption software used.		

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

Signed: _____

Date: _____

Appendix II: PERSONAL DATA REGISTER: Purpose and Lawfulness of Processing

The following table shows the categories of personal data processed by Links Childcare 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 our 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) Regulations 2016**
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**)
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 employment scheme	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

Review Dates:	June 2023		