## Document Control

### Document Number

| |
|---|
| LGTPOL003/2024 |

### Author

| Position | Name |
|---|---|
| Information & Reporting Officer | Jessie Shea |

### Stakeholders and Other Contributors

| Position | Name |
|---|---|
| External Consultant | Privacy Engine |

### Policy Origins

| New | Legacy |
|---|---|
| x | |

### Revision History

| Version | Issue Date | Author/Editor | Description/Summary of Changes |
|---|---|---|---|
| 1.0 | 28 August 2024 | Information & Reporting Officer | New |

### Reviewed By

| Version | Name | Position | Review Date |
|---|---|---|---|
| 1.0 | Katherine Harford | Executive Director | 11 September 2024 |
| 1.0 | Trish Hurley | Infant Mental Health and Wellbeing Coordinator | 11 September 2024 |
| 1.0 | Grace Walsh | Speech, Language and Early Years Coordinator | 11 September 2024 |

### Approvals

| Version | Issue Date | Approval Body | Approval Date | Effective Date |
|---|---|---|---|---|
| 1.0 | 12 September 2024 | Board of Directors | 19 September 2024 | 19 September 2024 |

## Data Retention & Erasure Policy

## Contents

## 1. Policy Statement

Let's Grow Together! Infant & Childhood Partnerships CLG (hereinafter referred to as the "Company") recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory, and regulatory obligations, to ensure the protection of personal information, and to enable the effective management of the organisation.

This policy and related documents meet the standards and expectations set out by contractual and legal requirements and has been developed to meet the best practices of business records management, with the aim of ensuring a structured approach to document control.

Effective and adequate records and data management are necessary to:

- Ensure that the business conducts itself in a structured, efficient and accountable manner
- Ensure that the business realises best value through improvements in the quality and flow of information and greater coordination of records and storage systems
- Provide services and programmes to families and other service providers and practitioners
- Support core business functions and provide evidence of conduct and the appropriate maintenance of systems, tools, resources and processes
- Meet legislative, statutory and regulatory requirements
- Deliver services to, and protect the interests of, employees, clients and stakeholders in a consistent and equitable manner
- Assist in document policy formation and managerial decision making
- Provide continuity in the event of a disaster or security breach
- Protect personal information and data subject rights
- Avoid inaccurate or misleading data and minimise risks to personal information
- Erase data in accordance with the legislative and regulatory requirements

Information held for longer than is necessary carries additional risk and cost and can breach data protection rules and principles. The Company only ever retains records and information for legitimate or legal business reasons and always comply fully with the data protection laws, guidance and best practice.

## 2. Purpose

The purpose of this document is to provide the Company's statement of intent on how it provides a structured and compliant data and records management system. 'Records' are defined as all documents, regardless of the format, which facilitate business activities, and are thereafter retained to provide evidence of transactions and functions. 'Business activities' include, but are not limited to: providing programmes and services to families and community members; providing training and capacity building to service providers and practitioners; engaging in monitoring, evaluation, and research activities both internally and with external partners; ongoing reporting activities; providing lectures, trainings, workshops, and other relevant activities to students at universities and other higher education institutions; providing placements for students; and advocacy activities.

Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

## 3. Scope

This policy applies to all staff within the Company (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, students, interns and agents engaged with the Company in Cork City, Ireland). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

## 4. Personal Information and Data Protection

The Company needs to collect personal information about the people we employ, work with, provide services to, and have a business relationship with to effectively and compliantly carry out our everyday business functions and activities, and to provide our programmes and services. This information can include (but is not limited to): name, contact information, date of birth, private and confidential information, sensitive information, medical information, and bank details.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to collecting, processing, storing and destroying all information in accordance with the General Data Protection Regulation, Ireland data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

Our Data Retention Policy and processes comply fully with the GDPR's fifth Article 5 principle:

*Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').*

## 5. Objectives

A record is information, regardless of media, created, received, and maintained which evidences the development of, and compliance with, regulatory requirements, business practices, legal policies, financial transactions, administrative activities, business decisions, or agreed actions. It is the Company's objective to implement the necessary records management procedures and systems which assess and manage the following processes:

- The creation and capture of records
- Compliance with legal, regulatory, and contractual requirements
- The storage of records
- The protection of record integrity and authenticity

- The use of records and the information contained therein
- The security of records
- Access to records
- Disposal/destruction of records

Records contain information that are a unique and invaluable resource to the Company and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information contained in them, as well as the individuals such information refers to. Records are also pivotal in the documentation and evidence of all business functions and activities.

The Company's objectives and principles in relation to Data Retention are to:

- Ensure that the Company conducts itself in an orderly, efficient, and accountable manner
- Support core business functions
- Provide evidence of compliant retention, erasure, and destruction
- Develop and maintain an effective and adequate records management system to ensure effective archiving, review, and destruction of information
- Only retain personal information for as long as is necessary
- Comply with the relevant data protection regulation, legislation, and any contractual obligations
- Ensure the safe and secure disposal of confidential data and information assets
- Mitigate against risks or breaches in relation to confidential information

## 6. Guidelines and Procedures

The Company manage records efficiently and systematically, in a manner consistent with the GDPR requirements. Records management training is mandatory for all staff as part of the Company's statutory and compliance training programme and this policy is widely disseminated to ensure a standardised approach to data retention and records management.

Records will be created, maintained, and retained to provide programmes and services, and provide information about and evidence of the Company's transactions, customers, employment, and activities. Records will be destroyed securely at the end of the specified retention period. Retention schedules will govern the period that records will be retained and describe the destruction at the end of the period, and can be found in the Retention Register – Data Retention Schedule at the end of this document.

It is our intention to ensure that all records and the information contained therein is:

- Accurate - records are reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document
- Accessible - records are made available and accessible when required
- Complete - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document
- Compliant - records always comply with any record keeping legal and regulatory requirements

- Monitored – staff, company, and system compliance with this Data Retention Policy is regularly monitored to ensure that the objectives and principles are being complied with at all times and that all legal and regulatory requirements are being adhered to

## 7. Retention Period Protocols

For all data and records obtained, used and stored within the Company, we:

- Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain
- Establish and verify retention periods for the data, with special consideration given to the below areas:
    - the requirements of the Company
    - the type of personal data
    - the purpose of processing
    - lawful basis for processing
    - the categories of data subjects
- Where it is not possible to define a statutory or legal retention period, as per the GDPR requirement, the Company will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices
- Have processes in place to ensure that records pending audit, litigation or investigation are not destroyed or altered
- For family and practitioner information obtained during the receipt of services: Transfer paper-based records and data to an electronic format

## 8. Suspension of Record Disposal for Litigation or Claims

If the Company is served with any legal request for records or information, any employee becomes the subject of an audit or investigation, or we are notified of the commencement of any litigation against our company, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

## 9. Destruction and Disposal of Records and Data

All information of a confidential or sensitive nature on paper or electronic media must be securely destroyed when it is no longer required. This includes the destruction of records at the end of the retention period. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees and clients.

The Company is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions of the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

## 10. Paper Records

The Company collects some personal information in a paper format. Family and practitioner / professional information will be transferred to an electronic version for storage and use. The paper version is securely shredded immediately after electronic transfer. The exception to this is that information collected in the Kidscope Paediatric Clinic is collected and stored in a paper format, and not transferred to an electronic version.

Company business information, including employee information, is stored in both paper and electronic format. It is stored in a secure and locked cabinet in a locked office.

The Company utilise onsite shredding to dispose of all routine paper materials. In some instances where there is a large amount of paper to be destroyed, an appropriate off-site shredding company will be commissioned.

## 11. Electronic Records

The Company collects some personal information electronically, and other information is collected in a paper format and transferred to an electronic format. Family and practitioner / professional information is stored and processed electronically. Company business information, including employee information, is stored in both paper and electronic format.

Information is stored on password-protected computers and mobile phones that are owned by the Company. All data is backed-up to the Cloud through Microsoft 365, which is managed by the designated IT Service Provider.

Personal data is securely and permanently deleted from the relevant computer or mobile, shared document, shared drive, and cloud storage.

## 12. IT Systems and Devices

The Company uses numerous systems, computers, mobile phones, and technology equipment in the running of our business. From time to time, such assets must be disposed of and due to the information held on these while they were active, this disposal is handled in an ethical and secure manner. Only the Executive Director can authorise the disposal of any IT equipment.

Where possible, information is wiped from the equipment through use of software and formatting, however this can still leave imprints or personal information that is accessible and so we also comply with the secure disposal of all assets. It is the explicit responsibility of the DPO to ensure that all relevant data has been sufficiently removed from the IT device and backed up before requesting disposal and/or prior to the scheduled pickup.

The designated IT service provider will be commissioned to wipe and dispose of IT devices.

## 13. Internal Correspondence and General Memoranda

Unless otherwise stated in this policy or the retention periods register, correspondence and internal memoranda should be retained for the same period as the document to which they pertain or support (i.e. where a memo pertains to a contract or personal file, the relevant retention period and filing should be observed).

Where correspondence or memoranda that do not pertain to any documents having already be assigned a retention period, they should be deleted or shredded once the purpose and usefulness of the content ceases or at a maximum of 7 years.

Examples of correspondence and routine memoranda include (but are not limited to): internal emails; meeting notes and agendas; general inquiries and replies; letters, notes, or emails of inconsequential subject matter.

## 14. Erasure

In specific circumstances, data subjects have the right to request that their personal data is erased, however the Company recognise that this is not an absolute 'right to be forgotten'. Data subjects only have a right to have personal data erased and to prevent processing if one of the below conditions applies:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully collected or processed
- The personal data must be erased in order to comply with a legal obligation

Where one of the above conditions applies and the Company received a request to erase data, we first ensure that no other legal obligation or legitimate interest applies. If we are confident that the data subject has the right to have their data erased, this is carried out by the DPO according to procedures outlined in our Data Protection Policy and Procedure, to ensure that all data relating to that individual has been erased.

These measures enable us to comply with a data subjects right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued storage and/or processing. While our standard procedures already remove data that is no longer necessary, we still follow a dedicated process for erasure requests to ensure that all rights are complied with, and that no data has been retained for longer than is needed.

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. Such refusals to erase data include:

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims
- If the data has been anonymised, collated, and shared (either with partner agencies or published publicly)

## 15. Special Category Data

In accordance with GDPR requirements, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the retention and erasure of

special categories of personal data.  Special Category Data that we collect, store, and process includes information that can identify racial or ethnic origin and health data.

Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, including Special Category Data.

## 16. Compliance and Monitoring

The Company are committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving and retention.

## 17. Responsibilities

The DPO must be involved in any data retention processes and records of all archiving and destructions must be retained. Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with the Company's policies and protocols.

The Executive Director retains overall responsibility for the management and oversight of all record and data collection, storage, processing, and destruction.

## 18. Review

This Policy will be reviewed biennially, or earlier as new information and/or legislation requires.

## Retention Register – Data Retention Schedule

| RECORD TYPE | REASON FOR COLLECTION AND RETENTION | RETENTION PERIOD | ACTION AT END OF RETENTION PERIOD |
|---|---|---|---|
| Information in individual family file (including contact details and demographic information) | To provide services, monitoring and evaluation | 7 years after the family closes with Let's Grow Together | Delete securely |
| Information in individual family file if it includes any information relating to Child Protection and Safety<br>* supersedes retention period of individual family file | To provide services | 14 years after the family closes with Let's Grow Together | Delete securely |
| Information on practitioner or professional (including contact details and demographic information) | To provide services, monitoring and evaluation | 7 years after the practitioner or professional stops working in the catchment area | Delete securely |
| Anonymised and collated family demographic information | Monitoring and evaluation | Indefinite | - |
| Anonymised and collated practitioner or professional demographic information | Monitoring and evaluation | Indefinite | - |
| Data specifically collected as part of an approved research project | To participate in the research project | Defined per project, as approved by our Research Approval Process | Delete securely |
| Kidscope information and records | To provide services | Until the patient's 25th birthday, or eight years after their death | Delete electronic records securely and confidentially shred paper records |
| Employee employment details | Legal obligation | 3 years after the employee resigns | Delete securely |
| Company financial information | Legal obligation | 6 years after the year the information relates to | Delete securely |
| Information collected during employment application process | Legal obligation | 1 year after close of employment post fulfilment | Delete securely |