Data Protection Policy

Version 1.0

Table of Contents

1. Executive Summary

This policy is to ensure that all information is retained in accordance with this policy, that all relevant care is taken to protect that information and to protect the personal data.

1.1 Scope

This policy covers

- All data recorded of a personal nature of any child and parent or carer.
- All data recorded of a personal nature of any colleague, student or person recruited.
- All data relating to the running of the business.

1.2 Out of Scope

Any item created by a child in their day-to-day care, education, and activities.

2. Access and Storage of Information Policy

It is the responsibility of every colleague to ensure that they are aware of the need to protect and deal with all data in accordance with this policy.
It is the responsibility of every colleague to ensure that all reasonable steps are taken to protect the data held.

Unless required all children will be known only by their first name, and this is the only form of identification that will be visible. For example, but not limited to Fire Registers, pictures and items created by the child, attendance registers.

All personal data will be retained for 6.5 years after the date a child leaves.

All personal data will only be shared with outside organisations where there is a need to share that information in either the care of the child or in the running of the business.
For example; sharing information with regulatory bodies (e.g. county council), those involved in medical care, or where for example payments are not made and the debt is passed to a 3rd Party.

Where there is a legal requirement provided to the business to provide information,

2.1 Storage of electronic data

All electric copies of data will only be kept in a relevant password protected directories or documents.
All reasonable steps will be taken to ensure that all portable computer equipment will be kept securely.
All computers that hold personal data will be left with the screen saver active and a password required to gain access.
Where data is required to be sent, relevant encryption and/or passwords will be used.

2.2 Storage or paper data

All paper documents will be kept when not in use in a locked filing system.
Where it is required to transport documents, these will be kept within a non-clear folder, and all reasonable steps taken to protect those.

2.3 Disposal of data

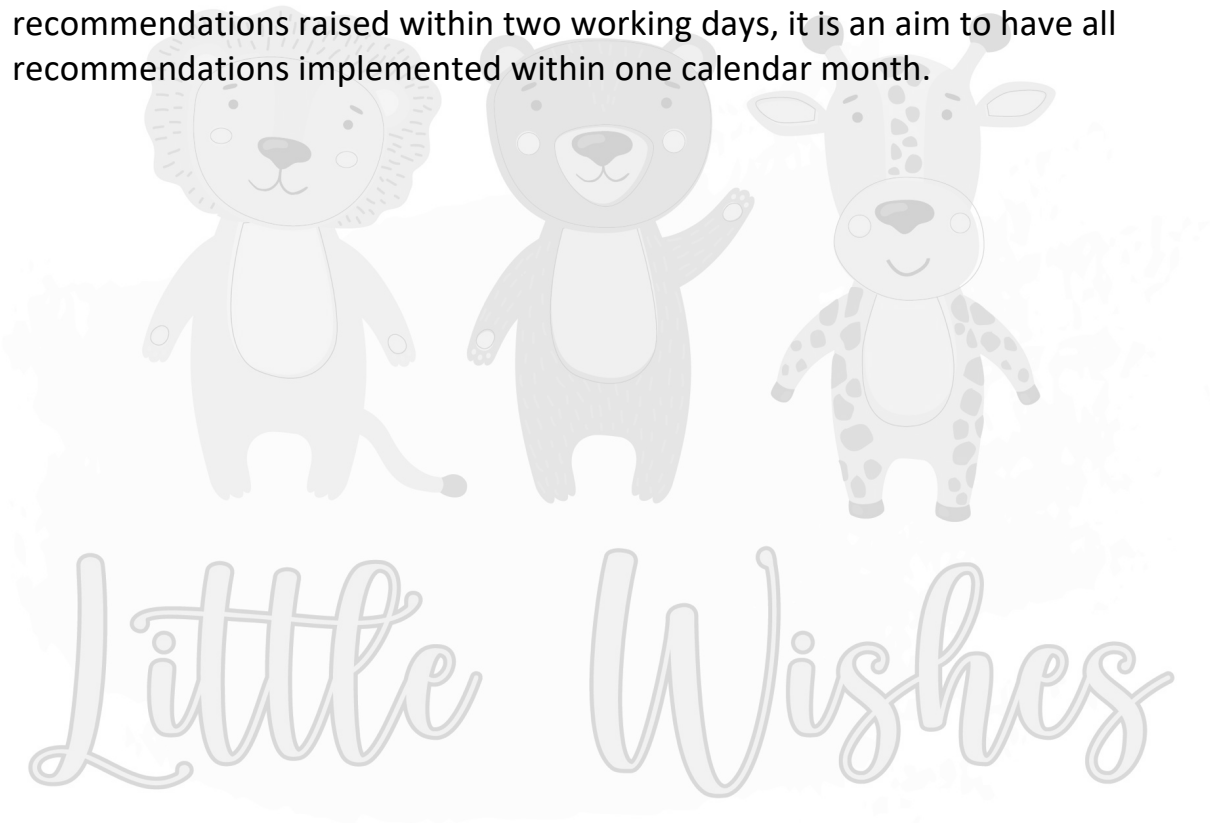
Where information is no longer required it will be securely disposed of.

2.4 Data Breech

Where it is suspected or reported that data security has been breached, this will be immediately informed to the Manager or Owner.

Where a breech has been reported the Manager or Owner will immediately instigate an investigation. Within 72 hours that investigation will be completed, and where a breech has been confirmed the Manager or Owner will inform the relevant individuals in writing. Where required formal reporting to the ICO will be made.

Where a response is received from the ICO, this will be reviewed and a list of recommendations raised within two working days, it is an aim to have all recommendations implemented within one calendar month.



2.5 Written in accordance with

The Statutory Framework for the Early Years Foundation Stage (2017) – Section 3:- Safeguarding and Welfare Requirements: Information and Records

"3.68. Providers must maintain records and obtain and share information (with parents and carers, other professionals working with the child, the police, social services and Ofsted or the childminder agency with which they are registered, as appropriate) to ensure the safe and efficient management of the setting, and to help ensure the needs of all children are met. Providers must enable a regular two-way flow of information with parents and/or carers, and between providers, if a child is attending more than one setting. If requested, providers should incorporate parents' and/or carers' comments into children's records.

3.69. Records must be easily accessible and available (with prior agreement from Ofsted or the childminder agency with which they are registered, these may be kept securely off the premises). Confidential information and records about staff and children must be held securely and only accessible and available to those who have a right or professional need to see them. Providers must be aware of their responsibilities under the Data Protection Act (DPA) 1998 and where relevant the Freedom of Information Act 2000.

3.70. Providers must ensure that all staff understand the need to protect the privacy of the children in their care as well the legal requirements that exist to ensure that information relating to the child is handled in a way that ensures confidentiality. Parents and/or carers must be given access to all records about their child, provided that no relevant exemptions apply to their disclosure under the DPA55.

3.71. Records relating to individual children must be retained for a reasonable period of time after they have left the provision."

3. Communicated Policy

Access and Storage of Information Policy

We take the security of all personal information extremely seriously, and It is the responsibility of every colleague to ensure that they are aware of the need to protect and deal with all data in accordance with this policy.
It is the responsibility of every colleague to ensure that all reasonable steps are taken to protect the data held.

Unless required all children will be known only by their first name, and this is the only form of identification that will be visible. For example, but not limited to Fire Registers, pictures and items created by the child, attendance registers.

All personal data will be retained for 6.5 years after the date a child leaves.
All personal data will only be shared with outside organisations where there is a need to share that information in either the care of the child or in the running of the business.
For example; sharing information with regulatory bodies (e.g. county council), those involved in medical care, or where for example payments are not made and the debt is passed to a 3rd Party.
Where there is a legal requirement handed to the business to provide information.

Storage of electronic data
All electric copies of data will only be kept in a relevant password protected directories or documents. All reasonable steps will be taken to ensure that all portable computer equipment will be kept securely. All computers that hold personal data will be left with the screen saver active and a password required to gain access.
Storage or paper data
All paper documents will be kept when not in use in a locked filing system.
Disposal of data
Where information is no longer required it will be securely disposed of

4. Appendix

4.1 Glossary of Terms

Accident	– Is an event that has resulted in an injury to one or more persons
Child / Children	– A young person who is a registered, or undertaking induction
Parent Carer	– Person responsible for the Child
Colleague	– Any employee, student or person recruited into a role.
Electronic data	– data stored on a computer, storage device or other electronic media
Paper Data	– data stored on a paper document
3rd Party	– Any organisation connected with the business or the services it provides.
Colleague	– Any employee, student or person recruited into a role.

4.2 Who is Responsible / RACI

		Owner	Manager	Finance	Office	Group Leader	Role	Role	Student		
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											

5. Document Control

5.1 Policy Review

This policy will be reviewed annually, any and all changes will be documented
Where there are no changes an entry confirming the review will be noted in the revisions.
Where an event occurs that dictates that the policy should be reviewed or amended, that will be undertaken as required.
All amendments and reviews should be signed by at least two stakeholders

5.2 Sign Off

Stakeholder	Role	Pages to Review (Optional)	Signature	Date
Katrina Higgins	Owner	All		22nd Feb 2023

5.3 Revisions

Version	Change Description	Sections	Date	Author	Reviewer
1.0	Initial Key process	All	22nd Feb 23	Katrina Higgins	Tim Higgins

This
Page
Is
Intentionally
Blank