Little Disciples Childcare

GDPR & Data Protection Policy

"Caring for children, supporting parents, and sparking imaginations – where quality, affordability, and excitement meet!"

Document Title:	GDPR & Data Protection Policy
Owner:	Little Disciples Childcare
Approval Date:	September 2024
Next Review Date:	September 2025
Distribution List:	Committee, Management Team, Staff & Parents
Responsible Individual Signature:	
Person in Charge Signature:	

Version	Date	Changes Made	Author	Approved By	Next Review Date
1.0	September 2023	Initial Release for Provider changes	S. Gocher	A. Stephens	Annually – September 2024
2.0	September 2024	Policy Review	S. Gocher	A. Stephens	Annually – September 2025
2.1	January 2025	Minor amendments – Pg numbers and Document Control	S. Gocher	A. Stephens	Annually – September 2025

Policy Statement

At Little Disciples Childcare, we are committed to providing a seamless and cohesive approach to childcare across all our services. This policy and procedure apply equally to both our Nursery Plus provision and our Breakfast, Afterschool, and Holiday Club services. This integrated framework ensures consistent standards of care, safety, and quality across all aspects of our provision, fostering a supportive and nurturing environment for every child in our care.

GDPR and Data Protection Policy

At Little Disciples Childcare, we respect the privacy of the children attending the setting and the privacy of their parents or carers, as well as the privacy of our staff. Our aim is to ensure that all those using and working at Little Disciples Childcare can do so with confidence that their personal data is being kept secure.

Our lead person for data protection is Mrs. Anna Stephens (Responsible Individual). The lead person ensures that the setting meets the requirements of the GDPR, liaises with statutory bodies when necessary, and responds to any subject access requests. Our designated Data Protection Officer (DPO) is Sarah Webb from e2e Consultancy.

Confidentiality

Within the setting, we respect confidentiality in the following ways:

- We will only ever share information with a parent about their own child.
- Information given by parents to the staff about their child will not be passed on to third parties without permission unless there is a safeguarding issue (as covered in our Safeguarding Policy).
- Concerns or evidence relating to a child's safety will be kept in a confidential file and will not be shared within the setting, except with the designated Child Protection Officer and the manager.
- Staff only discuss individual children for purposes of planning and group management.
- Staff are made aware of the importance of confidentiality during their induction process.
- Issues relating to the employment of staff, whether paid or voluntary, will remain confidential to those making personnel decisions.
- All personal data is stored securely in a lockable file, on a password-protected computer, passcode-locked phone, on a secure cloud-based program (OneDrive), or on our management software, which is password protected.
- Students on work placements and volunteers are informed of our Data Protection policy and are required to respect it.

Information that we keep

The items of personal data that we keep about individuals are documented on our personal data matrix. The personal data matrix is reviewed annually to ensure that any new data types are included.

Children and parents: We hold only the information necessary to provide a childcare service for each child. This includes child registration information, medical information, parent contact information, attendance records, incident and accident records, and so forth. Our lawful basis for processing this data is the fulfillment of our contract with the child's parents. Our legal condition for processing any health-related information about a child is so that we can provide appropriate care to the child. Once a child leaves our care, we retain only the data required by statutory legislation, insurance requirements, and industry best practices, and for the prescribed periods of time. Electronic data that is no longer required is archived, and paper records are disposed of securely after the required retention period.

Staff: We keep information about employees to meet HMRC requirements and to comply with all other areas of employment legislation. Our lawful basis for processing this data is to meet our legal obligations. Our legal condition for processing data relating to an employee's health is to meet the obligations of employment law. We retain the data after a member of staff has left our employment for the periods required by statutory legislation and industry best practices, then it is deleted or destroyed as necessary.

Data Minimization and Accuracy: We only collect the necessary personal data to fulfil our obligations. Steps are taken to ensure that all data we hold is accurate and up to date.

Data Breach Protocol

In the event of a data breach, we will:

- Take immediate steps to contain the breach and mitigate any potential impact.
- Assess the risks associated with the breach, including the potential harm to individuals.
- Notify affected individuals and the Information Commissioner's Office (ICO) within 72 hours if the breach poses a risk to individuals' rights and freedoms.
- Document the breach and actions taken to prevent future incidents.

Data Protection Impact Assessments (DPIA)

We will conduct Data Protection Impact Assessments (DPIAs) when introducing new technologies or processes that could significantly impact the privacy of individuals, to identify and mitigate risks.

Sharing information with third parties

We will only share child information with outside agencies on a need-to-know basis and with consent from parents, except in cases relating to safeguarding children, criminal activity, or if required by legally authorized bodies (e.g., Police, HMRC, etc.). If we decide to share information without parental consent, we will record this in the child's file, clearly stating our reasons.

We will only share relevant information that is accurate and up to date. Our primary commitment is to the safety and well-being of the children in our care.

Where we share relevant information where there are safeguarding concerns, we will do so in line with Government guidance 'Information Sharing Advice for Safeguarding Practitioners' (www.gov.uk).

Some limited personal information is disclosed to authorized third parties we have engaged to process it, as part of the normal running of our business, for example, in order to take online bookings, and to manage our payroll and accounts. Any such third parties comply with the strict data protection regulations of the GDPR. Our authorized third-party companies are:

- School iPal (Setting Management system)
- AVOW (Payroll Company)
- CPOMS (Safeguard monitoring software)
- Childcare Offer Portal (Welsh Government)
- Childcare Development Team (Flintshire County Council)

Data Transfers

If personal data needs to be transferred outside the European Economic Area (EEA), we ensure that appropriate safeguards are in place in accordance with GDPR requirements to protect the rights of the individuals involved.

Subject access requests

- Parents/carers can ask to see the information and records relating to their child, and/or any information that we keep about themselves.
- Staff and volunteers can ask to see any information that we keep about them.
- We will make the requested information available as soon as practicable and will respond to the request within one month at the latest.
- If our information is found to be incorrect or out of date, we will update it promptly.

- Parents/carers can ask us to delete data, but this may mean that we can no longer provide care to the child as we have a legal obligation to keep certain data. In addition, even after a child has left our care, we have to keep some data for specific periods, so we won't be able to delete all data immediately.
- Staff and volunteers can ask us to delete their data, but this may mean that we can no longer employ them as we have a legal obligation to keep certain data. In addition, even after a staff member has left our employment, we have to keep some data for specific periods, so we won't be able to delete all data immediately.
- If any individual about whom we hold data has a complaint about how we have kept their information secure, or how we have responded to a subject access request, they may complain to the Information Commissioner's Office (ICO).

Training and Awareness

All staff receive regular training and updates on data protection practices and GDPR compliance to ensure that they are aware of their responsibilities and the importance of protecting personal data.

Retention Schedule

A data retention schedule is in place to ensure that personal data is not held for longer than necessary. Data is regularly reviewed and securely disposed of when no longer required.

Contact Details

For any data protection concerns or requests, individuals can contact:

- **Data Protection Officer (DPO):** Sarah Webb, e2e Consultancy
- **Information Commissioner's Office (ICO):**

GDPR

We comply with the requirements of the General Data Protection Regulation (GDPR) regarding obtaining, storing, and using personal data.