Data Protection Policy

At Stride360, we respect the privacy of the children attending our sessions, their parents or carers, and our staff. We are committed to ensuring that personal data is handled securely and in compliance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy outlines how we manage, protect, and use personal data effectively.

Confidentiality

At Stride360, 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 Stride360 staff about their child will not be passed on to third parties without permission unless there is a safeguarding issue (as outlined in our Safeguarding Policy).
- Concerns or evidence relating to a child's safety will be kept in a confidential file and only shared within Stride360 with the Designated Safeguarding Lead (DSL) 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, or a passcode-locked phone.

Information We Keep

Students 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, and incident and accident records.
- Once a child leaves our care, we retain only the data required by statutory legislation and industry best practice for prescribed periods. Electronic data that is no longer required is deleted, and paper records are securely disposed of.

Staff:

- We keep information about employees to meet HMRC requirements and comply with employment legislation. Information is retained after a staff member has left for the recommended period and then securely deleted or destroyed.

Lawful Basis for Processing

Stride360 processes personal data under the following lawful bases:

- Consent: For optional data collection (e.g., marketing communications).
- Contract: To fulfill contractual obligations (e.g., payroll processing).
- Legal Obligation: To meet statutory requirements (e.g., HMRC reporting).
- Legitimate Interests: To support business operations while respecting individual rights.

Data Protection Officer (DPO)

Simone Lyons is the appointed Data Protection Officer (DPO) for Stride360. She is responsible for overseeing GDPR compliance and handling any data protection queries or concerns.

Data Sharing with Third Parties

- We only share child information with outside agencies on a need-to-know basis and with consent from parents unless required by law (e.g., safeguarding, criminal investigations).
- If we share information without parental consent, the reasons will be recorded in the child's file. Only relevant, accurate, and up-to-date information will be shared.
- Limited personal information may be disclosed to authorized third parties engaged by Stride360 (e.g., payroll and accounts services), who comply with GDPR regulations.

Subject Access Requests

- Parents/carers can request to see information held about their child or themselves.
- Staff and volunteers can request to see information held about them.
- Requested information will be made available promptly, within one month at the latest.
- If information is found to be incorrect or outdated, it will be promptly updated.
- Complaints about how data is handled can be directed to the ICO.

Data Breach Procedure

In the event of a data breach:

- The breach will be assessed immediately to determine its scope and impact.
- If the breach poses a risk to individuals' rights, the ICO will be notified within 72 hours.
- Affected individuals will be informed promptly where required.
- All incidents will be documented, including corrective actions taken to mitigate risks.

Staff Training

- All staff receive GDPR training during induction and annual refresher sessions to stay updated on compliance requirements.
- Training covers data protection principles, recognizing potential breaches, and handling personal data securely.

Retention Policy

- Specific retention periods are applied to different categories of data in line with statutory requirements. For example:
    - Child registration and medical information: Retained for the duration of care and statutory requirements thereafter.
    - Employment records: Retained for six years after employment ends.
- Data is securely deleted or destroyed when no longer needed.

Privacy Notices

Stride360 provides clear privacy notices to all stakeholders, outlining how their personal data is collected, used, stored, and shared. These notices ensure transparency and compliance with GDPR requirements.

GDPR Compliance

Stride360 complies with the requirements of the General Data Protection Regulation (GDPR), ensuring all personal data is:

- Processed lawfully, fairly, and transparently.
- Collected for specified, explicit, and legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Stored securely and retained only as long as necessary.

This policy was adopted by Stride 360	Date: 10/01/25
To be reviewed by: 10/01/26	Written by: Simone Lyons