FIRST STEPS TOGETHER
FOR EVERY JOURNEY

DATA PROTECTION POLICY

Revision History			
Date	**Version**	**Change**	**Author**
April 26	**2**	**Policy updated**	**E Burgess N Ledger**

1. Aims
First Steps Together ensures all personal data relating to pupils, families, staff, visitors and partners is collected, used, stored and disposed of in line with the UK GDPR and Data Protection Act 2018. This policy applies to all formats of personal data, including paper and digital records.

2. Legislation and Guidance
This policy is based on:

- UK GDPR
- Data Protection Act 2018
- ICO guidance on data protection, CCTV and subject access requests
- Education (Pupil Information) (England) Regulations 2005
-

3. Definitions
Key terms include:

- **Personal data:** Information identifying an individual (e.g., name, ID number, location data).
- **Special category data:** Sensitive information requiring extra protection (e.g., health, ethnicity, biometrics).
- **Processing:** Any action involving personal data.
- **Data subject:** The individual the data relates to.
- **Data controller:** Determines how and why data is processed.
- **Data processor:** Processes data on behalf of the controller.
- **Personal data breach:** Any accidental or unlawful loss, disclosure or destruction of personal data.
-

4. Data Controller
First Steps Together is the data controller for all personal data processed within the organisation.

5. Roles and Responsibilities
5.1 Data Protection Officer (DPO)
Deena Ledger (data@firststepstogether.uk) oversees compliance, advises on data protection matters, and is the first point of contact for individuals and the ICO.

5.2 All Staff
Staff must:

- Collect, use and store personal data in line with this policy
- Report concerns, breaches or uncertainties to the DPO
- Seek advice before sharing data externally
- Follow security procedures at all times

Failure to comply may result in disciplinary action.

6. Data Protection Principles
Personal data must be:

- Lawful, fair and transparent
- Collected for specific purposes
- Adequate, relevant and limited
- Accurate and up to date
- Kept only as long as necessary
- Secure at all times

7. Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

We process data only where a lawful basis applies, including:

- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests
- Consent

Special category data is processed only where an additional condition applies.

7.2 Minimisation and Accuracy

We collect only what is necessary, keep it accurate, and delete it when no longer required.

8. Sharing Personal Data

We share data only when necessary and lawful, including:

- Safeguarding or safety concerns
- Liaison with external agencies
- Use of approved suppliers/contractors
- Legal requirements (e.g., police, local authority, courts)
- Emergency situations

All third-party processors must meet GDPR standards.

9. Subject Access Requests (SARs)

Individuals may request access to their personal data. Requests must be forwarded immediately to the DPO.

We respond within one month unless the request is complex. We may refuse or charge a fee if the request is excessive or repetitive.

Pupil SARs

Children aged 12+ are usually considered competent to make their own requests, unless assessed otherwise.

10. Parental Requests for Educational Records

Parents of pupils under 18 may request access to their child's educational record. We respond within 15 working days.

11. CCTV

CCTV is used for safety and security. Signs clearly indicate where recording takes place. Use complies with ICO guidance.

12. Photographs and Videos

We obtain written parental consent before using images for communication, marketing or online publication. Consent can be withdrawn at any time.

Images are never accompanied by identifying personal information.

13. Data Security and Storage of Records

We protect personal data from unauthorised access, loss or damage. Key measures include:

- Paper records and portable devices stored securely when not in use

- Confidential papers never left unattended
- Sign-in/out procedures for data taken off-site
- Strong passwords and encryption on all devices
- Staff using personal devices must follow the same security standards

Secure Handling of Printed Personal Data
Personal data should be viewed digitally wherever possible. Printing is permitted **only when absolutely necessary**.
Where printing is unavoidable:

- The individual who prints the data ("the printee") is **fully responsible** for its security from printing to shredding
- Printed personal data must remain **in the printee's direct possession and control at all times**
- It must never be left unattended or stored insecurely
- All printed personal data must be **shredded immediately after use** using approved confidential waste methods

Failure to follow these requirements may constitute a data breach. If printed data is lost or accessed by an unauthorised person, an investigation will take place and may result in disciplinary action.

14. Disposal of Records
Personal data is disposed of securely when no longer required. Approved third-party disposal services must meet GDPR standards.

15. Personal Data Breaches
All suspected breaches must be reported immediately to the DPO. The DPO will investigate, contain the breach, assess risk, notify affected individuals where required, and report to the ICO within 72 hours if necessary.
A full breach response procedure is included in Appendix 1.

16. Training
All staff receive data protection training at induction and refresher training when legislation or procedures change.

17. Monitoring
The DPO reviews this policy annually or sooner if legislation changes.

APPENDIX 1
PERSONAL DATA BREACH REPORTING FORM

1. Basic Information
Date of report:
Time of report:
Name of person reporting the breach:
Job role:
Contact details:
How did you become aware of the breach? (Brief description)

2. Description of the Incident
Date and time the breach occurred (if known):
Location of the breach:
Describe what happened: (Include a clear, factual summary of the incident)

Type of breach (tick all that apply):

- ☐ Loss of data
- ☐ Theft
- ☐ Unauthorised access
- ☐ Accidental disclosure
- ☐ Sending information to the wrong person
- ☐ Technical/system failure
- ☐ Printed data left unsecured
- ☐ Other (please specify): _____

3. Personal Data Involved
What categories of personal data were affected? (e.g., names, addresses, medical information, safeguarding information, staff data)

Was any special category (sensitive) data involved?

- ☐ Yes
- ☐ No If yes, specify: _____

Approximate number of individuals affected:
Approximate number of records affected:

4. How the Data Was Stored or Shared
Format of the data involved:

- ☐ Printed paper
- ☐ Email
- ☐ Laptop/PC

- ☐ Mobile device
- ☐ USB/portable media
- ☐ Cloud system
- ☐ Other: _____

Was the data encrypted or password protected?

- ☐ Yes
- ☐ No
- ☐ Not applicable

5. Containment Actions Taken

What immediate steps have been taken to contain the breach? (e.g., email recall, device locked, data retrieved, password reset)

Has the data been recovered?

- ☐ Yes
- ☐ No
- ☐ Partially

Has anyone else been informed (e.g., ICT, manager)?

- ☐ Yes
- ☐ No If yes, who: _____
-

6. Potential Impact

What risks or harm may result from this breach? (e.g., distress, reputational damage, identity theft, safeguarding concerns)

Are any individuals at immediate risk?

- ☐ Yes
- ☐ No If yes, describe: _____

7. DPO Section (to be completed by the Data Protection Officer)

DPO Name: Deena Ledger

Date received:

Assessment

- Is this a personal data breach under UK GDPR?
  - ☐ Yes
  - ☐ No
- Is the breach likely to result in a risk to individuals' rights and freedoms?
  - ☐ Yes
  - ☐ No
- Is ICO notification required?
  - ☐ Yes
  - ☐ No If yes, date reported to ICO: _____
- Is notification to affected individuals required?
  - ☐ Yes

- ☐ No If yes, date completed: _____

Actions Taken

(Containment, mitigation, communication, recovery)

Lessons Learned / Preventative Measures

(Training, policy changes, technical controls)

DPO Signature:

Date: