Interactive Learning Diary Ltd
(inc Interactive Nursery Manager)
Data Processing Agreement
1st March 2025

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement, unless the context otherwise requires:

- **"Data Protection Laws"** means all applicable laws relating to the processing of Personal Data including the UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations 2003, and any successor legislation.
- **"Controller"**, **"Processor"**, **"Data Subject"**, **"Personal Data"**, **"Personal Data Breach"**, **"Processing"** and **"Supervisory Authority"** shall have the meanings given in the UK GDPR.
- **"Services"** means the Interactive Learning Diary (ILD) and/or Interactive Nursery Manager (INM) software services and related hosting services provided by the Processor to the Controller as set out in Schedule 1.
- **"Sub-processor"** means any third party appointed by the Processor to process Personal Data on behalf of the Controller.
- **"ILD"** means Interactive Learning Diary software for capturing observations and assessments.
- **"INM"** means Interactive Nursery Manager software for nursery management operations.

2. BACKGROUND AND SCOPE

2.1 The Controller operates nursery services and requires the Processor to provide software and data hosting services for managing child records, staff information, and parent communications.

2.2 In providing the Services, the Processor will process Personal Data on behalf of and on the documented instructions of the Controller.

2.3 This Agreement sets out the terms on which the Processor will process Personal Data on behalf of the Controller in accordance with Article 28 of the UK GDPR.

2.4 The parties agree that the Controller is the Data Controller, and the Processor is the Data Processor in respect of the Personal Data processed under this Agreement.

2.5 The Processor provides:

- Software platform (ILD and/or INM) for data entry, storage, retrieval and management
- Secure cloud hosting infrastructure
- Backup and restore services
- Technical support and maintenance
- Parent portal services

3. PROCESSING INSTRUCTIONS

3.1 The Processor shall process Personal Data only on documented instructions from the Controller, unless required to do so by applicable law.

3.2 The Controller's instructions are set out in:

- This Agreement and its Schedules
- The Services Agreement between the parties
- The Controller's use of the ILD/INM software platform functionality
- Any additional written instructions provided by the Controller from time to time

3.3 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes Data Protection Laws.

3.4 The Processor shall not process Personal Data for any purpose other than as instructed by the Controller.

3.5 The subject matter, duration, nature and purpose of the processing, the types of Personal Data and categories of Data Subjects are set out in Schedule 1.

3.6 The Processor acknowledges that the Controller has sole responsibility for:

- Determining what Personal Data to collect and enter into the system
- Obtaining appropriate consent from data subjects
- Providing privacy notices to data subjects
- Responding to data subject rights requests
- Determining lawful bases for processing

4. PROCESSOR'S OBLIGATIONS

4.1 The Processor shall:

(a) Process Personal Data only in accordance with the Controller's documented instructions.

(b) Ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) Take all measures required pursuant to Article 32 of UK GDPR (security of processing) as detailed in Schedule 2;

(d) Respect the conditions for engaging another processor as set out in Section 6.

(e) Taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as possible, for the fulfilment of the Controller's obligation to respond to requests for exercising Data Subject rights under Chapter III of UK GDPR.

(f) Assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of UK GDPR, taking into account the nature of processing and information available to the Processor.

(g) At the choice of the Controller, delete or return all Personal Data to the Controller after the end of the provision of services relating to processing, and delete existing copies unless applicable law requires storage of the Personal Data.

(h) Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of UK GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

4.2 The Processor shall immediately inform the Controller if it believes that any instruction violates Data Protection Laws.

4.3 The Processor shall not use Personal Data for any marketing purposes.

5. SECURITY MEASURES

5.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

5.2 The security measures currently implemented by the Processor are set out in Schedule 2. The Processor may update these measures from time to time provided that the level of security is not reduced.

5.3 Such measures shall include, as appropriate:

(a) The pseudonymisation and encryption of Personal Data (the Processor uses AES-256 encryption).

(b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

(c) The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident (daily backups with offsite storage).

(d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.4 The Processor shall ensure that access to Personal Data is limited to those personnel who require access to perform the Services.

6. SUB-PROCESSING

6.1 The Controller provides general authorisation for the Processor to engage Sub-processors for the provision of the Services.

6.2 The Processor shall:

(a) Maintain a current list of Sub-processors, which is set out in Schedule 3.

(b) Provide the Controller with at least 30 days' prior written notice of the addition or replacement of any Sub-processor.

(c) Provide the Controller with reasonable information regarding the Sub-processor to enable the Controller to exercise its right to object.

6.3 The Controller may object to the Processor's appointment or replacement of a Sub-processor on reasonable grounds relating to data protection within 14 days of notification. If the Controller objects, the parties shall discuss in good faith with a view to achieving a commercially reasonable resolution.

6.4 Where the Processor engages a Sub-processor, the Processor shall:

(a) Enter into a written contract with the Sub-processor imposing on the Sub-processor the same data protection obligations as are imposed on the Processor under this Agreement.

(b) Remain fully liable to the Controller for the performance of the Sub-processor's obligations.

6.5 Any Sub-processor engaged by the Processor must comply with the same standards set out in the Processor's Data Protection Policy and this Agreement.

7. DATA SUBJECT RIGHTS

7.1 The Processor shall, taking into account the nature of the processing, provide reasonable assistance to enable the Controller to respond to requests from Data Subjects exercising their rights under Chapter III of UK GDPR, including:

(a) Right of access (Article 15)

(b) Right to rectification (Article 16)

(c) Right to erasure (Article 17)

(d) Right to restriction of processing (Article 18)

(e) Right to data portability (Article 20)

(f) Right to object (Article 21)

7.2 If the Processor receives a request from a Data Subject directly, it shall forward the request to the Controller without undue delay and in any event within 2 working days of receipt. The Processor shall not respond to Data Subject requests without the Controller's prior written authorisation.

7.3 The Processor's assistance shall include:

(a) Providing the Controller with access to relevant Personal Data held in the system

(b) Providing data exports in secure PDF format or other machine-readable formats

(c) Implementing any rectifications, deletions, or restrictions instructed by the Controller within the timeframes required by Data Protection Laws

7.4 The Processor shall respond to Controller requests for assistance within the timeframes necessary for the Controller to comply with its obligations under Data Protection Laws (typically within 5 working days to allow the Controller to respond within the statutory one-month period).

8. PERSONAL DATA BREACHES

8.1 The Processor shall notify the Controller without undue delay and in any event within 24 hours upon becoming aware of a Personal Data Breach affecting the Controller's Personal Data.

8.2 The notification shall be sent to the Controller's designated contact (as notified to the Processor) and shall, at a minimum, include:

(a) A description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects and Personal Data records concerned.

(b) The name and contact details of the Processor's Data Protection Officer: Justin Evans, 03452241172 / 07795326790 (24/7) justin.evans@interactivelearningdiary.co.uk

(c) A description of the likely consequences of the Personal Data Breach.

(d) A description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

8.3 The Processor shall provide all reasonable cooperation and assistance to the Controller in relation to any Personal Data Breach, including:

(a) Investigating the breach and providing regular updates.

(b) Mitigating and remedying the breach.

(c) Providing information and documentation to assist the Controller in notifying the Supervisory Authority and Data Subjects where required.

(d) Responding to enquiries from Data Subjects, Supervisory Authorities or other third parties as directed by the Controller.

8.4 The Processor shall not inform any third party of a Personal Data Breach without the Controller's prior written consent, except as required by law or to Sub-processors as necessary to investigate and remediate the breach.

8.5 The Processor maintains a breach notification procedure as detailed in Part 29 of its Data Protection Policy, ensuring all breaches are reported immediately to Justin Evans, Data Protection Officer, who will coordinate the response.

9. DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

9.1 The Processor shall provide reasonable assistance to the Controller with any Data Protection Impact Assessments and prior consultations with Supervisory Authorities that the Controller is required to carry out under Articles 35 and 36 of UK GDPR.

9.2 Such assistance shall include providing the Controller with:

(a) Information about the technical and organisational measures implemented by the Processor (as detailed in Schedule 2).

(b) Information about Sub-processors and their processing activities (Schedule 3).

(c) Details of security measures and risk assessments.

(d) Information about data retention periods and disposal methods.

(e) Any other information reasonably requested by the Controller.

10. DELETION OR RETURN OF DATA

10.1 Upon termination or expiry of the Services, the Processor shall, at the Controller's written election:

(a) Return all Personal Data to the Controller in secure PDF format or other structured, commonly used and machine-readable format; and/or

(b) Securely delete all Personal Data in accordance with the methods set out in Part 6 of the Processor's Data Retention Policy.

10.2 **Standard Retention Period:** Where the Controller does not provide specific instructions, the Processor shall:

(a) Retain the Controller's data for a period of **3 months** following termination or non-renewal to allow for data retrieval.

(b) Provide the Controller with written notice 30 days before final deletion.

(c) After the 3-month period, permanently delete all Personal Data using:

- **Electronic data:** Gutmann (35 pass) secure deletion method

- **Hardcopy Data Disposal:**

  - **Standard:** Shredded to Level 3 (P-4) - particles 4mm x 60mm
  - **Special Category:** Shredded to Level 4 (P-5) - particles 2mm x 15mm, or incinerated with certificate

- **Physical Media Disposal:** Hard drives, USB drives: Securely wiped (minimum 3 passes) or physically destroyed. Certificate obtained from disposal contractors.

10.3 The Processor shall provide written certification to the Controller that it has completed the deletion or return of Personal Data within 7 days of completion.

10.4 The Processor may retain Personal Data to the extent required by applicable law, provided that the Processor ensures the confidentiality of such Personal Data and only processes it as necessary to comply with the legal requirement.

10.5 All backups containing Personal Data shall be deleted in accordance with the same secure methods within 90 days of termination, subject to technical limitations of backup rotation cycles.

11. AUDIT RIGHTS

11.1 The Processor shall allow the Controller (or its authorised representatives or independent auditors) to audit the Processor's compliance with this Agreement and Data Protection Laws.

11.2 The Controller may conduct such audits:

(a) Once per calendar year upon reasonable written notice (not less than 30 days).

(b) At any time without notice where the Controller reasonably believes there has been a Personal Data Breach or non-compliance with this Agreement.

11.3 Audits shall be conducted during normal business hours (9am-5pm Monday-Friday excluding public holidays) and shall not unreasonably interfere with the Processor's business operations.

11.4 The Controller shall ensure that its auditors are bound by appropriate confidentiality obligations.

11.5 The Processor may charge reasonable costs for facilitating audits.

11.6 If an audit reveals non-compliance with this Agreement, the Processor shall, at its own cost, take all necessary corrective action without undue delay and provide the Controller with a written remediation plan within 14 days.

12. INTERNATIONAL TRANSFERS

12.1 The Processor confirms that all Personal Data processing occurs within the United Kingdom. The Processor shall not transfer Personal Data outside the United Kingdom without the Controller's prior written consent.

12.2 Current Data Locations:

- **Primary hosting:** Fasthosts Internet Limited servers located at Discovery House, 154 Southgate Street, Gloucester, GL1 2EX, United Kingdom
- **Backup storage:** Microsoft Azure datacentre located in Cardiff, United Kingdom
- **No international transfers occur**

12.3 If the Processor proposes to transfer Personal Data outside the UK in the future (including through use of new Sub-processors), the Processor shall:

(a) Provide at least 60 days' advance written notice to the Controller.

(b) Implement appropriate safeguards under Article 46 of UK GDPR (such as UK International Data Transfer Agreement or Standard Contractual Clauses).

(c) Obtain the Controller's prior written consent.

(d) Provide the Controller with all information necessary to demonstrate that appropriate safeguards have been implemented.

12.4 The Controller may refuse consent to any proposed international transfer on reasonable data protection grounds.

12.5 In accordance with Part 28 of the Processor's Data Protection Policy, any international transfers would only proceed if they met the strict criteria set out in UK GDPR Articles 45-46.

13. TERM AND TERMINATION

13.1 Commencement and Duration

This Agreement shall commence on the Effective Date and shall continue in full force and effect for so long as the Processor Processes Personal Data on behalf of the Controller (the "**Term**"), unless terminated earlier in accordance with this Clause 13.

13.2 Termination for Material Breach

13.2.1 Either Party may terminate this Agreement by giving **thirty (30) days' written notice** to the other Party if the other Party:

a) Commits a material breach of any provision of this Agreement; and

b) In the case of a breach capable of remedy, fails to remedy such breach within **thirty (30) days** of receiving written notice specifying the breach and requiring its remedy.

13.2.2 Material breaches include, but are not limited to:

a) Any breach of Clause 5 (Security Measures).

b) Any unauthorised disclosure or use of Personal Data.

c) Failure to notify a Personal Data Breach in accordance with Clause 8.

d) Unauthorised engagement of a Sub-processor in breach of Clause 9.

e) Failure to provide cooperation and assistance as required under Clause 7.

f) Repeated or persistent breaches of this Agreement, even if individually remedied.

g) Any breach that results in regulatory enforcement action by the ICO or other supervisory authority.

13.3 Termination for Insolvency

Either Party may terminate this Agreement immediately by written notice if the other Party:

13.3.1 Becomes insolvent, enters into administration, receivership, liquidation, or any similar proceedings.

13.3.2 Makes any arrangement or composition with its creditors.

13.3.3 Ceases or threatens to cease to carry on business.

14.3.4 Is unable to pay its debts as they fall due within the meaning of Section 123 of the Insolvency Act 1986.

13.4 Termination Without Cause

Either Party may terminate this Agreement by giving the other Party **ninety (90) days' written notice** without cause, provided that such termination shall not take effect until all Personal Data has been deleted or returned in accordance with Clause 10.

13.5 Effect of Termination

13.5.1 Upon termination or expiry of this Agreement for any reason:

a) The Processor shall immediately cease all Processing of Personal Data except to the extent necessary to comply with Clause 10 (Deletion or Return of Personal Data).

b) The Processor shall comply with Clause 10 within **thirty (30) days** of the effective date of termination, unless the Controller requests an extended timeframe in writing.

c) The Processor shall provide written certification to the Controller that it has complied with its obligations under Clause 10.

d) Each Party shall return or securely destroy all Confidential Information of the other Party, except to the extent required to be retained by law.

e) The Processor shall cooperate with the Controller to ensure a smooth transition of services and shall provide reasonable assistance to facilitate the Controller's migration to an alternative processor.

13.5.2 Termination or expiry of this Agreement shall not affect any rights, remedies, obligations, or liabilities of either Party that have accrued up to the date of termination or expiry.

13.5.3 The Controller shall pay the Processor for all Processing services properly performed and all reasonable costs incurred up to the effective date of termination.

14. GENERAL PROVISIONS

14.1 Entire Agreement

14.1.1 This Agreement, together with the schedules and appendices attached hereto, constitutes the entire agreement between the Parties relating to the Processing of Personal Data and supersedes all prior agreements, arrangements, understandings, representations, and warranties (whether written or oral) relating to such subject matter.

14.1.2 This Agreement shall be read in conjunction with and forms part of:

a) The Processor's Data Protection Policy

b) The Processor's Data Retention Policy

14.1.3 In the event of any conflict or inconsistency between the provisions of this Agreement, the provisions of this Agreement shall prevail to the extent of such conflict or inconsistency with respect to the Processing of Personal Data.

14.1.4 Each Party acknowledges that it has not relied on any statement, representation, warranty, or understanding which is not expressly set out in this Agreement.

14.2 Amendments and Variations

14.2.1 No amendment, modification, or variation of this Agreement shall be effective unless it is made in writing and signed by duly authorised representatives of both Parties.

14.2.2 The Processor may update its Data Protection Policy and Data Retention Policy from time to time to reflect changes in Data Protection Laws, best practices, or operational requirements. The Processor shall:

a) Notify the Controller of any material changes to such policies at least **thirty (30) days** in advance of implementation.

b) Provide the Controller with a copy of the updated policies.

c) Allow the Controller to object to such changes within **fourteen (14) days** of notification if the changes would materially adversely affect the Controller's rights or obligations.

d) If the Controller objects, the Parties shall negotiate in good faith to resolve the objection. If resolution cannot be achieved within **thirty (30) days**, either Party may terminate this Agreement in accordance with Clause 13.4.

14.2.3 Changes required to comply with Data Protection Laws shall be implemented immediately upon the Processor providing notice to the Controller, and the Controller's consent shall not be required.

14.3 Severability

14.3.1 If any provision of this Agreement is held to be invalid, illegal, or unenforceable by any court or regulatory authority of competent jurisdiction:

a) Such provision shall be deemed modified to the minimum extent necessary to make it valid, legal, and enforceable while preserving its intent; or

b) If such modification is not possible, the provision shall be deemed deleted from this Agreement.

14.3.2 The invalidity, illegality, or unenforceability of any provision shall not affect the validity, legality, or enforceability of the remaining provisions, which shall continue in full force and effect.

14.3.3 If any provision is deemed deleted pursuant to Clause 14.3.1(b), the Parties shall negotiate in good faith to agree upon a valid, legal, and enforceable substitute provision that achieves the same or similar economic effect as the deleted provision.

14.4 Waiver

14.4.1 No failure or delay by either Party in exercising any right or remedy under this Agreement shall constitute a waiver of that right or remedy or preclude its exercise at any subsequent time.

14.4.2 No single or partial exercise of any right or remedy shall preclude any other or further exercise of that or any other right or remedy.

14.4.3 Any waiver of any breach of this Agreement shall not be deemed to be a waiver of any subsequent breach.

14.4.4 A waiver shall only be effective if given in writing and signed by the waiving Party.

14.5 Assignment and Subcontracting

14.5.1 The Controller may assign, transfer, or otherwise dispose of its rights and obligations under this Agreement without the Processor's consent, provided that the assignee agrees in writing to be bound by the terms of this Agreement.

14.5.2 The Processor may not assign, transfer, or otherwise dispose of its rights or obligations under this Agreement without the prior written consent of the Controller, such consent not to be unreasonably withheld or delayed.

14.5.3 The engagement of Sub-processors by the Processor shall be governed by Clause 6 (Sub-processing) and not by this Clause 14.5.

15.5.4 This Agreement shall be binding upon and inure to the benefit of the Parties and their respective successors and permitted assigns.

14.6 Third Party Rights

14.6.1 Except as expressly provided in this Agreement, no person who is not a party to this Agreement shall have any right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.

14.6.2 Data Subjects are express third-party beneficiaries of Clauses 5 (Security Measures), 7 (Data Subject Rights), 8 (Personal Data Breaches), and 10 (Deletion or Return of Data), and may enforce these provisions directly against the Processor.

14.7 Notices

14.7.1 Any notice or other communication required or permitted to be given under this Agreement shall be in writing and shall be:

a) Delivered personally.

b) Sent by recorded delivery or registered post.

c) Sent by email to the addresses specified below (or such other address as notified by one Party to the other).

d) For urgent data breach notifications, sent by telephone followed by written confirmation.

14.7.2 Controller's notice details:

Address: [**INSERT CONTROLLER'S REGISTERED ADDRESS**]
Email: [**INSERT CONTROLLER'S DPO EMAIL**]
Attention: Data Protection Officer

14.7.3 Processor's notice details:

Address: Forest View House, 7, Blair of Tarradale, Muir of Ord, IV6 7PY, United Kingdom
Email: justin.evans@interactivelearningdiary.co.uk
Telephone: 0345 224 1172
Attention: Justin Evans, Data Protection Officer

14.7.4 Notices shall be deemed received:

a) If delivered personally, at the time of delivery.

b) If sent by recorded delivery or registered post, two (2) Business Days after posting.

c) If sent by email, at the time of transmission (provided no delivery failure notification is received).

14.8 Governing Law and Jurisdiction

14.8.1 This Agreement and any dispute or claim arising out of or in connection with it (including non-contractual disputes or claims) shall be governed by and construed in accordance with the **laws of Scotland.**

14.8.2 The Parties irrevocably agree that the **courts of Scotland** shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement (including non-contractual disputes or claims).

14.8.3 Nothing in this Clause 14.8 shall limit the right of either Party to bring proceedings for injunctive relief or other equitable remedies in any jurisdiction.

14.9 Compliance with Processor's Policies

14.9.1 The Processor shall Process Personal Data in accordance with:

a) This Data Processing Agreement.

b) All lawful instructions from the Controller.

c) Data Protection Laws.

d) The Processor's **Data Protection Policy** (1st March 2025).

e) The Processor's **Data Retention Policy** (1st March 2025).

f) All applicable industry standards and best practices.

14.9.2 The Processor represents and warrants that its Data Protection Policy and Data Retention Policy comply with UK GDPR and Data Protection Laws and implement appropriate technical and organisational measures as required by Article 32 UK GDPR.

14.9.3 Copies of the Processor's current Data Protection Policy and Data Retention Policy are available upon request from the Data Protection Officer at justin.evans@interactivelearningdiary.co.uk.

14.9.4 The Processor shall ensure that all personnel authorised to Process Personal Data are subject to appropriate confidentiality obligations and have received adequate training on Data Protection Laws and the requirements of this Agreement.

14.10 Counterparts

This Agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute an original, but all counterparts together shall constitute one and the same instrument. Delivery of an executed counterpart by email (PDF) or other electronic means shall be effective as delivery of a manually executed counterpart.

SCHEDULE 1: DETAILS OF PROCESSING

Subject Matter: ILD/INM cloud software for nursery operations

Duration: Services Agreement term + 3 months post-termination

Nature & Purpose: Host/store data, provide software tools, generate reports, facilitate parent communications, process payments, backup/restore, technical support

Types of Personal Data:

- **Child:** Names, DOB, addresses, photos, medical info, allergies, dietary needs, emergency contacts, attendance, development notes, special needs, safeguarding

- **Parent/Guardian:** Names, addresses, phones, emails, employment, payment info, bank details, NI numbers (for funding)
- **Staff:** Names, addresses, DOB, NI number, DBS checks, qualifications, employment records, reviews, salary, bank details, absence

Categories of Data Subjects: Children (0-5 years), Parents/guardians, Staff, Emergency contacts, Authorised collectors

SCHEDULE 2: TECHNICAL AND ORGANISATIONAL MEASURES

1. Access Control: MFA, RBAC, unique credentials, 15-min timeout, lockout after 5 fails, 12+ char passwords, 90-day changes

2. Encryption: AES-256 at rest/in transit, TLS 1.3+, encrypted backups, 7-Zip for email transfers

3. Network Security: Firewalls, IDS monitoring, patching (48hrs critical), secure networks only

4. Physical Security: ISO 27001 datacentres (Gloucester & Cardiff UK), 24/7 monitoring.

5. Backup: Daily backups (evening GMT), Microsoft Azure Cardiff, 90-day retention, encrypted, quarterly restore testing, RTO/RPO: 24hrs

6. Logging: Audit logs, 12-month retention, real-time monitoring, tamper-proof storage

7. Vulnerability Management: Annual pen testing, secure SDLC, code reviews, WAF protection

8. Incident Response: 24/7 monitoring, breach notification procedures, 24-hour Controller notification

9. Data Minimisation: Collect only necessary data, automated deletion per retention schedules, privacy-by-design

SCHEDULE 3: LIST OF SUB-PROCESSORS

Sub-processor	Location	Activity	Safeguards
Fasthosts Internet Limited	Gloucester, UK	Infrastructure hosting, data storage	UK-based, ISO 27001 / ISO 9001 / ISO 50001 no international transfer
Microsoft Azure	Cardiff, UK	Secure backup storage	UK-based, ISO 27001/27018, no international transfer

Note: Processor provides 30 days' notice before Sub-processor changes. Controller may object within 14 days.

SCHEDULE 4: INTERNATIONAL DATA TRANSFERS

Current Position: NO INTERNATIONAL TRANSFERS

All processing occurs in UK (Gloucester & Cardiff). Processor confirms no data transfers outside UK.

Future Changes: 60 days' notice, appropriate safeguards (UK IDTA/SCCs), Controller consent required.

SIGNATURES

For nursery / school (Data Controller):

Signed: _____

Name: _____

Position: _____

Date: _____

For Interactive Learning Diary Ltd (Data Processor):

Signed: _____

Name: _____

Position: _____

Date: _____