Data Processing Agreement (For schools)

V 3.3 (June 2026)

This Data Processing Agreement (the '**Agreement**') forms part of the terms of the Services and the Subscription Agreement between the Education Institution and the Licensor (each as identified in the Information Table below), in connection with their selected education programs and products.

Information Table

Education Institution	**Detail**
School / Education Institution	As set out in the Subscription Agreement
Address	As set out in the Subscription Agreement
Email	As set out in the Subscription Agreement
Program(s) / Product(s)	As set out in the Subscription Agreement (including trial subscriptions as applicable)
Effective Date	[ ] If blank, applies from the commencement date in the Quote.

Background

The Education Institution acts as a Data Controller and wishes to procure the Services from the Licensor, which involve the processing of personal information.

From the Effective Date, the Parties agree to implement a data processing arrangement that complies with applicable Data Protection Laws (as defined below).

1. Definitions and Interpretation

Unless otherwise defined in this Agreement, capitalised terms used in this Agreement have the meaning given to them below.

'Agreement' means this Data Processing Agreement and all Annexures.

'Child' / 'Children' means an individual under the age at which valid consent to digital services can be given in the Education Institution's jurisdiction. For these products, that includes: under 13 years of age under COPPA and PIPEDA; under 16 years under the UK GDPR digital-services consent age; under the age set by the relevant EU Member State under Article 8 of the EU GDPR (13 to 16); under 15 years of age in the Australian schools and home context as informed by the OAIC Children's Online Privacy Code; and under the age at which consent is valid under other applicable laws.

'Data Protection Laws' means, as applicable to the jurisdiction of the Education Institution and the Services, the UK GDPR and the Data Protection Act 2018; the EU GDPR (Regulation 2016/679); the Australian Privacy Act 1988 and the Australian Privacy Principles (APPs); the New Zealand Privacy Act 2020; the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA); the South African Protection of Personal Information Act (POPIA); applicable US federal and state laws including FERPA (20 USC §1232g), COPPA (including the FTC COPPA Rule and the Final Rule published 22 April 2025), SOPIPA, and CCPA/CPRA where applicable..

'Data Transfer' means (a) a transfer of Education Institution Personal Data from the Education Institution to the Licensor; or (b) an onward transfer of Education Institution Personal Data from the Licensor to a Subprocessor, including in each case where the transfer crosses a national or regional border that engages a cross-border transfer obligation under any Data Protection Law.

'EEA' means the European Economic Area.

'Education Institution' means the school, school district, multi-academy trust, local authority, or other education organisation named in the Information Table as the Controller of the Personal Data processed under this Agreement.

'Education Institution Personal Data' means any Personal Data Processed by the Licensor or a Subprocessor on behalf of the Education Institution under or in connection with the Subscription Agreement.

'Licensor' means the contracting 3P Learning group entity for the Services in the Education Institution's region, being (as applicable): 3P Learning UK Limited for the UK and EEA; 3P Learning Limited or 3P Learning Australia Pty Limited for Australia and New Zealand; 3P Learning Inc. for the United States; 3P Learning Canada Limited for Canada; or such other 3P Learning group entity identified in the Subscription Agreement.

'Non-Integral Disclosure' means a disclosure of a Child's personal information to a third party that is not necessary to deliver the Services (for example, advertising, data brokerage, or AI or machine-learning model training outside of the educational service). Non-Integral Disclosures require separate, opt-in parental consent.

'Persistent Identifier' means technical data including cookies, device identifiers, IP addresses, log data and similar identifiers that can be used to recognise a user or device over time.

'Processing' / 'Process' means has the meaning given in the applicable Data Protection Laws; the Processing activities under this Agreement are set out in Annexure A Part 2.

'Program Security Requirements' means the technical and organisational security measures set out in Annexure A Part 3.

'Services' means the services and data processing to deliver the learning programs and their ancillary services as listed in Annexure A Part 1 and as further described in the Subscription Agreement.

'Subprocessor' means any person, including any 3P Learning group company other than the Licensor, appointed from time to time by or on behalf of the Licensor to Process Personal Data on behalf of the Education Institution in connection with this Agreement. The list of these entities can be found in the Subprocessor Reference Document published at www.3plearning.com/privacy.

'Subscription Agreement' means the quotation and purchase agreement entered by the Education Institution for the Services, including the term of the product subscription and the number of users.

The terms 'Commission', 'Controller', 'Data Subject', 'Member State', 'Personal Data', 'Personal Data Breach', 'Processing' and 'Supervisory Authority' have the meanings given to them under the applicable Data Protection Laws.

2. Processing of Education Institution Personal Data

2.1. The Licensor shall:

- comply with all applicable Data Protection Laws in the Processing of Education Institution Personal Data;

- not Process Education Institution Personal Data other than in accordance with this Agreement, the documented instructions of the Education Institution, the Subscription Agreement and applicable law; and
- safeguard Education Institution Personal Data to standards not less than the Program Security Requirements.

2.2. The Education Institution instructs the Licensor to Process Education Institution Personal Data only for the purposes described in Annexure A Part 2.

2.3. The Licensor is responsible to the Education Institution for the Licensor's and each Subprocessor's compliance with the applicable Data Protection Laws.

2.4. Where Education Institution Personal Data relates to Children, the Licensor shall apply the additional controls set out in section 12 of this Agreement.

3. Licensor Personnel

The Licensor shall take reasonable steps to ensure that:

- Education Institution Personal Data is only used as strictly necessary to perform the Services under the Subscription Agreement or as expressly authorised by the Education Institution;
- access to Education Institution Personal Data is limited to those employees, agents and Subprocessors who need to access such data to perform the Services and to comply with applicable law; and
- each such employee, agent or Subprocessor is subject to appropriate written confidentiality undertakings.

4. Security

4.1. Taking into account industry standards, 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 Licensor shall implement appropriate technical and organisational measures to ensure security capability and controls appropriate to that risk in relation to Education Institution Personal Data. Those measures include the Program Security Requirements in Annexure A Part 3 and the requirements of Article 32(1) of the UK GDPR and EU GDPR, APP 11 of the Australian Privacy Principles, section 19 of POPIA, and the safeguarding principle of PIPEDA Schedule 1, in each case where applicable.

4.2. In assessing the appropriate level of security, the Licensor shall take account of the risks presented by Processing, in particular the risk of a Personal Data Breach.

4.3. Where the Processing involves Children's data, the Licensor shall also apply: independent penetration testing at least annually for all customer-facing products that process Children's data; mandatory annual children's privacy training for all employees with access to such data; and a documented incident response plan that is reviewed at least annually and that includes notification obligations to customers and relevant authorities.

5. Subprocessing

5.1. The Education Institution acknowledges that the list of Subprocessors may be updated from time to time. The current list, including their function, data types processed and jurisdiction, is published and maintained at www.3plearning.com/privacy.

5.2. The Licensor shall give the Education Institution at least 30 days' prior written notice (which may be given by email, or by an update to the Subprocessor Reference Document with notification, to the Education Institution's nominated contact) before adding or replacing a Subprocessor. During that notice period, the Education Institution may object on reasonable data-protection grounds by notifying us at privacy@3plearning.com. If we are unable resolve the objection in good faith within a further 30 days, we may restore or limit Services to the agreed processing or discuss solutions, including termination by the Education Institution.

5.3. The Licensor shall not appoint, or disclose Education Institution Personal Data to, any Subprocessor except in accordance with this section 5 or as otherwise authorised by the Education Institution.

5.4. The Licensor shall enter data-protection terms with each Subprocessor that provide at least the same level of protection for Education Institution Personal Data as those in this Agreement, and remains responsible to the Education Institution for the performance of each Subprocessor's obligations.

6. Data Subject Rights

6.1. The Licensor shall support the Education Institution in fulfilling Data Subject rights as required by Data Protection Laws, including the rights of access, correction, restriction, objection, data portability, and erasure (the right to be forgotten).

6.2. The Licensor shall apply appropriate technical and organisational measures, and give reasonable to enable the Education Institution to respond to requests to exercise Data Subject rights under Data Protection Laws.

6.3. The Licensor shall: (a) promptly notify the Education Institution if it receives a request from a Data Subject under any Data Protection Law in respect of Education Institution Personal Data; and (b) not respond to that request except on the documented instructions of the Education Institution or as required by applicable law (in which case the Licensor shall, to the extent permitted by law, inform the Education Institution of that legal requirement before responding).

6.4. The Licensor does not make solely automated decisions from Education Institution Personal Data in respect of Children that produce legal effects or similarly significant effects.

7. Personal Data Breach

7.1. The Licensor shall notify the Education Institution without undue delay, and in any event within 48 hours, of becoming aware of a Personal Data Breach affecting Education Institution Personal Data, to the extent then known. If full details are not available within the 48-hours, the Licensor shall provide the initial notification and supplement it without further undue delay and in any event within 72 hours of becoming aware. For Education Institutions in the UK and EEA, the information provided shall align with Article 33(3) of the UK GDPR and EU GDPR.

7.2. The Licensor shall co-operate with the Education Institution and take such reasonable commercial steps as are directed by the Education Institution to assist in the investigation, mitigation and remediation of each such Personal Data Breach, and shall maintain a written record of each Personal Data Breach affecting Education Institution Personal Data. It remains the duty of the Education Institution to notify regulators as the data controller.

8. Data Protection Impact Assessment

8.1. The Licensor shall provide reasonable assistance to the Education Institution with any data protection impact assessments, and any consultations with Supervisory Authorities or other competent data protection authorities, which the Education Institution reasonably considers to be required under relevant Data Protection Law.

8.2. The Licensor shall conduct its own Data Protection Impact Assessments before launching new features that materially affect the Processing of Children's personal information, and shall consult with the relevant Supervisory Authority where a residual high risk is identified.

9. Deletion or Return of Education Institution Personal Data

9.1. Subject to this section 9, the Licensor shall, within 30 days of the date of the Education Institution's written request (the **'Request Date'**), delete or irreversibly anonymise all copies of the Education Institution Personal Data, excluding limited records held in back-up systems ('Back-up Records') which are not generally accessible and necessary for security, resilience and business continuity measures. The Licensor shall take reasonable steps to remove, overwrite or de-identify Back-up Records in accordance with the back-up retention period in Annexure A Part 4.

9.2. The Licensor shall provide written certification to the Education Institution that it has complied with this section 9 within 30 days of the Request Date.

9.3. An Education Institution may submit a request to remove Educational Institution Personal Data at any time to privacy@3plearning.com.

10. Audit Rights

10.1. On the Education Institution's reasonable written request, the Licensor shall make available all information reasonably necessary to demonstrate compliance with this Agreement in relation to the Processing of Education Institution Personal Data by the Licensor or any Subprocessor.

10.2. For Educational Institutions in the UK and EEA, the audit scope may include verification of compliance with Articles 28 to 32 of the UK GDPR and EU GDPR (and equivalent provisions of other applicable Data Protection Laws), and may take the form of summaries, certifications, reports and where reasonably necessary on-site inspection.

10.3. Audits are subject to: (a) at least 30 days' prior written notice (except in the case of a confirmed Personal Data Breach or regulatory inquiry, where a shorter period may apply); (b) no more than one audit in any 12-month period, except in the case of a confirmed Personal Data Breach or regulatory inquiry; (c) the auditor being subject to written confidentiality undertakings of equivalent standard to those in section 17; (d) the audit being conducted during business hours of the Licensor and in a manner that does not unreasonably disrupt the Services; (e) measures to prevent any access to other customers' data or information that would create a security vulnerability in the Services; and (f) the Education Institution bearing the reasonable costs of the audit, unless the audit reveals a material breach of this Agreement solely attributable to the Licensor, in which case the Licensor shall bear those costs.

11. International Data Transfers

11.1. The Licensor may transfer Education Institution Personal Data to a country outside the Education Institution's home jurisdiction only where an appropriate safeguard for that transfer is in place under applicable Data Protection Laws and as set out in this Agreement and Annexure A Part 2.

11.2. The Education Institution consents to the Licensor and its Subprocessors Processing Education Institution Personal Data in the countries listed in Annexure A Part 2, subject to the safeguards set out in this section 11.

11.3. The following transfer mechanisms apply by origin jurisdiction:

- UK / EU / EEA: the EU Standard Contractual Clauses and the UK International Data Transfer Addendum (IDTA) or UK International Data Transfer Agreement, as applicable, supplemented by appropriate technical and organisational measures.
- Australia: contractual safeguards which require the overseas recipient to handle the personal information in a way consistent with the Australian Privacy Principles, as required by APP 8.1.

- New Zealand: a written agreement with the overseas recipient that provides comparable safeguards to the New Zealand Privacy Act 2020, consistent with IPP 12.
- Canada: contractual measures ensuring a comparable level of protection by the third party, consistent with PIPEDA Schedule 1 clause 4.1.3.
- United States: contractual measures consistent with FERPA, COPPA, SOPIPA and applicable state student privacy laws, and the EU/UK SCC framework where data also engages those regimes.
- South Africa: contractual measures consistent with section 72 of POPIA.

11.4. Educational Institutions can request additional information on the specific transfer mechanism applicable to the Education Institution's data flows by contacting privacy@3plearning.com.

12. Children's Data and Specific Regulatory Commitments

12.1. This section applies to the Personal Data of Children provided by the Educational Institution to the Licensor under the Subscription Agreement:

12.2. **Permitted uses.** The Licensor shall Process Children's personal information only to deliver the educational service the Education Institution has requested. The Licensor shall not use Children's personal information for behavioural advertising, profiling for third parties, training of artificial intelligence or machine learning models, or any Non-Integral Disclosure.

12.3. **Persistent Identifiers.** Persistent Identifiers collected from Children are used only for the internal operations of the Services (authentication, security, diagnostics, service reliability, internal analytics and legal compliance). The Licensor shall not export Persistent Identifiers to advertising or profiling platforms and shall ensure that Subprocessors are contractually prohibited from using Persistent Identifiers for such purposes.

12.4. **Biometric, government-issued identifiers and geolocation.** The Licensor does not collect biometric identifiers (such as voiceprints, facial templates or fingerprints), government-issued identifiers (such as social security numbers, passport numbers or birth certificates) or precise or coarse geolocation data from Children or any other users for identification or tracking purposes. Voice recordings may be processed solely for the Read Aloud reading fluency feature in school subscriptions, to enable the teacher to assess and grade student reading, and are retained for the period set out in Annexure A Part 4.

12.5. **FERPA and US student privacy.** Where the Licensor provides services to schools, school districts or education agencies in the United States, the Licensor agrees to act as a 'school official' with a legitimate educational interest under FERPA (20 USC §1232g) and to use student education records only to provide the Services under the school's direction. The Licensor complies with COPPA (including the FTC COPPA Final Rule of 22 April 2025), SOPIPA and applicable state student privacy laws.

12.6. **Australian Children's Online Privacy Code.** For services provided in Australia, the Licensor will review its policies and practices to align with the OAIC Children's Online Privacy Code, and with any obligations under the Online Safety Act 2021 (Cth) applicable to its products.

12.7. **Separate choice.** An Education Institutions consent for the Licensor to collect and use student personal information to deliver the Services does not constitute consent to any Non-Integral Disclosure of that data. The Licensor and its related companies do not currently make Non-Integral Disclosures of Children's personal information. Any proposal to do so will be communicated to the Education Institution in advance of implementation and will not proceed without separate, documented authorisation.

13. Prohibited Processing

13.1. The Licensor warrants that it does not and will not:

- sell Education Institution Personal Data to advertisers or any other third party, whether in personal, anonymous or aggregated form;
- engage in targeted or behavioural advertising to Children using Education Institution Personal Data;
- use Children's personal information to build profiles of Children for cross-service use or for any third party's own purposes;
- disclose or transfer Education Institution Personal Data to third parties except as authorised by the Education Institution or as set out in this Agreement; or
- use Children's personal information to train artificial intelligence or machine learning models.

13.2. The Licensor and its related companies may use irreversibly anonymised data (which is no longer personal data) for the development and improvement of the Services.

14. Persistent Identifiers

14.1. The Licensor uses Persistent Identifiers solely to support the internal operations of the Services: authenticating users; security and fraud prevention; troubleshooting and diagnostics; service reliability and performance; internal analytics and A/B testing; and compliance and record-keeping.

14.2. Security logs containing Persistent Identifiers are retained by the Licensor for 12 months and are then deleted. The Licensor shall implement technical controls, including role-based access control, network segmentation, logging and review of platform and application logs by relevant teams, to prevent Persistent Identifiers from being exported to advertising or profiling platforms.

15. Notice of Significant New Processing Purposes

If the Licensor proposes to use Education Institution Personal Data for a purpose that is materially different from what is described in this Agreement, the Subscription Agreement or the 3P Learning Privacy Policy during the subscription term, the Licensor shall: (a) notify the Education Institution in advance; (b) explain the new purpose, basis of processing, any new recipients and any new retention period; and (c) obtain new instructions from the Education Institution before the new use begins. The Educational Institution agrees that the notifications may be received from notices, including notices in the Product for the features or options, and containing the processing information for user acceptance.

16. Data Ownership

16.1. The Education Institution retains ownership of, and remains Data Controller of, all student and teacher personal information Processed under this Agreement.

16.2. Student-generated content and results are owned by the Education Institution and its students. The Education Institution authorises the Licensor to (a) use this content to deliver the Services, including for features such as progress tracking, reporting and feedback to the Educational Institution in accordance with this Agreement, and (b) anonymise the content for the Licensor’s product development, quality control and research or educational purposes.

16.3. The Licensor owns the underlying platform, software and any irreversibly anonymised insights derived from any use of the Services. Where data has been irreversibly anonymised it is no longer personal data and is not governed by this Agreement.

17. General Terms

17.1. **Confidentiality.** Each party must keep this Agreement, and information it receives about the other party and its business in connection with this Agreement ('Confidential Information'), confidential, and must not use or disclose that Confidential Information without the prior written consent of the other party except to the extent that (a) disclosure is required by law or by a regulator with jurisdiction over the disclosing party, or (b) the relevant information is already in the public domain other than through breach of this Agreement.

17.2. **Notices.** All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post, or sent by email to the address set out in the Document Control section of this Agreement (or such other address as notified in writing, including under the Subscription Agreement).

17.3. **Precedence.** If there is any inconsistency between this Agreement and any other document referenced in it (including the 3P Learning Privacy Policy and the Retention Periods reference), this Agreement prevails in respect of school-managed Processing under this Agreement.

18. Dispute Resolution

18.1. Any dispute arising in connection with this Agreement must be notified in writing to the other party. The Education Institution and Licensor shall have 20 business days from the date of that notice to endeavour to resolve the dispute in good faith.

18.2. To notify us of a dispute, please contact our 3P Learning Data Privacy Office: privacy@3plearning.com

18.3. Any dispute not resolved under the preceding paragraph shall be referred to and finally resolved by arbitration under the UNCITRAL Arbitration Rules. The seat of arbitration shall be the capital city of the governing law jurisdiction. The language of the arbitration shall be English. The tribunal shall consist of one arbitrator unless the parties agree otherwise. Nothing in this section limits a party's right to seek urgent equitable or injunctive relief from a court of competent jurisdiction.

19. Governing Law

The governing law of this Agreement is determined by the location of the Education Institution, as follows:

- Education Institutions located in the United Kingdom: the laws of England and Wales.
- Education Institutions located in the European Economic Area: the laws of Ireland.
- Education Institutions located in Australia: the laws of New South Wales, Australia.
- Education Institutions located in New Zealand: the laws of New Zealand.
- Education Institutions located in Canada: the laws of the Province of Ontario, Canada.
- Education Institutions located in the United States: the laws of the State of New York.
- Education Institutions located in South Africa: the laws of the Republic of South Africa.
- Education Institutions located elsewhere: the laws of England and Wales, unless the Subscription Agreement specifies otherwise.

Annexure A

Part 1: Services and Products

This Agreement covers the following Licensor products, as applicable per the Subscription Agreement :

Product	Scope
Mathletics	Mathematics learning, assessment and reporting

Reading Eggs / Reading Eggspress	Reading and literacy program
Mathseeds	Early years mathematics
Writing Legends	Writing program
LiteracyPlanet	English literacy
Brightpath Progress	Writing assessment and moderation (School only)

The Services delivered across the products listed in the Subscription Agreement include:

- e-learning program delivery, in-program learning features, reporting and hosting;
- responding to customer enquiries;
- providing user guidance, account management and support tickets;
- reporting and e-learning resources for teachers;
- administering class rostering, including integrations where available and requested; and
- product analytics, performance diagnostics and feature optimisation in the delivery of the above.

Part 2: Personal Data Categories and Processing Activities

Categories of individual and categories of personal data Processed:

Category of individual	**Categories of personal data**
Students (pupils)	First name and last name or initials, year or grade level, school name, class assignment, login ID, learning activity data (scores, progress, time on task, content interactions, free-text entered into learning activities, and Read Aloud voice feature for school subscriptions only).
Teachers	Name, work email, school name, role, login ID, support correspondence.
School administrators	Name, work email and contact details, school name, role, login ID, licence allocation information, support correspondence.
All users (technical)	Persistent Identifiers including IP address, device or browser type, authentication logs, system access patterns and security logs, used for the internal operations of the Services only (see section 14).

Processing activities carried out by the Licensor on the Education Institution's instructions:

Processing activity	**Data involved**
Account creation and user settings (teachers, administrators, students)	Names, usernames, roles, school details, authentication logs.
Class rostering and integration with school systems	Student names or initials, class assignments, student identifier.
Teacher dashboards and reporting	Student activity data.
Usage analysis and reporting to the school	Aggregated and student-level usage data.

Data anonymisation or export, on verified school request	Student, teacher and activity data.
Support requests directed from the school	User identifiers, support correspondence.
Product updates and newsletters to teachers	Teacher data.
Learning, assessment and content delivery	Student activity data.
Read Aloud activity feature (Reading Eggs school subscriptions only)	Student audio recording for teacher assessment; retained per Annexure A Part 4 to enable teacher grading across the academic year.
Program activity leaderboards	Student first name and initial, activity score; no full name displayed publicly.
Hosting of program data	Student, teacher, activity data, user identifiers.
Platform security, abuse prevention, audit logging	Persistent Identifiers, security logs.
Data retention for service delivery	Student, teacher, activity data, user identifiers.
Improving educational programs (product development)	Irreversibly anonymised usage, activity and engagement data only.
Optional: participation in educator communities of practice	Teacher and school data; opt-in basis only.
Optional: participation in events or competitions (for example, World Maths Day)	Student first name and initial, school, activity data; opt-in basis only.

Subprocessors. The Subprocessors listed below process Education Institution Personal Data in connection with the Services. The current version of this list is published at www.3plearning.com/privacy and is updated in accordance with section 5. Other 3P Learning group entities (as listed in the 3P Learning Privacy Policy) may act as Subprocessors and are bound by intra-group data processing terms equivalent to those in this Agreement.

Subprocessor	Service	Purpose	Storage location	Student data shared
Amazon Web Services (AWS)	Cloud hosting	Secure hosting of platforms and data	Australia, US, EU	Yes (hosting)
Microsoft Azure	Cloud services	Application hosting and operations	US, EU	Yes (hosting)
Microsoft 365	Communications	Email, document storage	AU, US	No
Cloudflare	CDN and security	Performance and protection	Global	Transit only
Apple App Store	App distribution	Mobile app distribution	US	No
Google Play Store	App distribution	Mobile app distribution	US	No

Hotjar (anonymised configuration)	Product analytics	Service improvement insights	EU / US	No
Salesforce / Marketing Cloud	CRM and marketing	School Support, Account management and marketing (consent)	AU / US	No
ClassLink / Clever / Wonde	School-directed rostering	Receiving school roster data (B2B only)	US / UK / Global	Yes (B2B only, school-directed)
Ortto	CRM marketing (LiteracyPlanet)	Teacher marketing CRM and campaign tracking.	AU	No

Part 3: Program certification and registration information

Security certifications and registrations:

Product	**Certification**
Mathletics, Reading Eggs, Mathseeds, Writing Legends	SOC 2 Type 2
Reading Eggs and Mathseeds	kidSAFE+ COPPA Certified Seal (US)
Mathletics, Reading Eggs, Mathseeds, Writing Legends, LiteracyPlanet, Brightpath Progress	Safer Technologies for Schools (ST4S) (AU and NZ)
3P Entity	**Registration**
3P Learning UK Limited	UK ICO Registration: Z2188515

Encryption:

Product	**Standard**
Mathletics, Reading Eggs, Mathseeds, Writing Legends, Brightpath Progress	AES-256 at rest; TLS 1.2 or higher in transit.
LiteracyPlanet	SHA-256 at rest; TLS 1.2 or higher in transit.

Technical and organisational measures:

Measure	**Implementation**
Pseudonymisation and encryption	Users may elect to use pseudonyms. AES-256 at rest, TLS 1.2 or higher in transit.

Confidentiality, integrity, availability and resilience	Least-privilege access, role-based access control (RBAC), single sign-on (SSO) and multi-factor authentication (MFA) for mission-critical applications, and regular penetration testing and assurance audits.
Restoration of availability after incident	Documented incident response plan, reviewed annually, including parental and regulator notification obligations.
Testing and evaluating technical measures	Regular vulnerability scanning and assurance audits. For child-facing products, independent penetration testing at least annually.
User identification and authorisation	MFA and RBAC. Network segmentation between production, corporate and development environments.
Protection of data during storage	Cloud hosting (AWS, Azure) with relevant security certifications. Encrypted backups used for disaster recovery only.
Endpoint protection	Anti-malware, disk encryption and device management on all employee devices with access to children's data.
Physical security	Access-controlled offices, password-protected systems and secure Wi-Fi.
Events logging	Platform and application logs are captured under documented protocols and reviewed by relevant teams. Security logs are retained for 12 months and then deleted.
IT security governance	Documented IT and security policies, with executive accountability under the Chief Technology Officer and oversight by the Risk Management function reporting to the Audit and Risk Committee.
Staff training	Mandatory annual cybersecurity training, and specific children's privacy training for all employees with access to children's data.
Data minimisation	Only the minimum personal information required to deliver the feature is collected. Pseudonymity is available where customers prefer.
Data quality	Education Institutions and parent customers administer their own account details. The Licensor responds promptly to data quality questions.
Data portability and erasure	Deletion or irreversible anonymisation within 30 days of a verified request. Export of data is available on verified school request.
Privacy by design and default	Data Protection Impact Assessments conducted before higher-risk Processing and before substantial changes. Child-impact assessments are conducted before launching features that materially affect Children.

Part 4: Data Retention

For school-managed (B2B) accounts, (i) school expiry is typically triggered by the end of a school's licence or contract with 3P Learning; (ii) school student accounts expiry is generally initiated via the user

roster lifecycle, specifically through student or teacher activity and roster status; should a student be deleted from the roster, the account transitions to inactive status following a six-month grace period.

In the table below 'account expiry', has the meaning given in the 3P Learning Privacy Policy: The point at which a user account becomes inactive.

School Subscriptions (B2B):

Data category	Purpose of collection	Business need for retention	Retention period
Teacher Account Credentials (name, email, username, password)	Maintain account and provide access	School annualised reporting requirements	Expired school licences: anonymised 18 months after account expiry. Active school licences: anonymised 6 months after removal from roster.
Student Rostering (name, grade, class)	Provide access to educational activities and content	School annualised reporting requirements	Expired school licences: anonymised 18 months after account expiry. Active school licences: anonymised 6 months after removal from roster.
Student Gameplay and Activity data (scores, progress, inventory, avatars, free-text entries)	Maintain child's progress and experience in app	School annualised reporting requirements	Expired school licences: anonymised 18 months after account expiry. Active school licences: anonymised 6 months after removal from roster.
Voice Recording (Read Aloud feature)	For teachers to assign and evaluate students' reading capabilities and progress	Enable teacher to grade student reading across a maximum academic year of 24 months	Deleted after 24 months.
Customer Support Records (emails, chat logs, tickets)	Resolve user issues and improve service quality	Quality assurance, dispute resolution, and analysis of recurring bugs	Deleted 24 months after the date of ticket closure.

Encrypted backups are retained for up to 18 months for recovery and year-on-year reporting, and are not generally accessible except for business continuity.

On-request deletion: on receipt of a verified request, the Licensor will irreversibly anonymise the relevant Education Institution Personal Data from production systems within 30 days. Early removal requests may be submitted at any time via privacy@3plearning.com.

Anonymisation follows the 3P Learning Data Anonymisation Standard, ensuring irreversible removal of personal identifiers, that no re-identification is technically or reasonably possible, and that the data cannot be linked back to an individual.

Precedence. This Annexure Part 4 is aligned with the 3P Learning Privacy Reference - Retention Periods document. In case of inconsistency between this Annexure and any other 3P Learning retention reference document, this Annexure prevails for school-managed Processing under this Agreement.

Part 5: Supervisory Authorities by Jurisdiction

Jurisdiction	Supervisory Authority
UK	Information Commissioner's Office (ICO): ico.org.uk; icocasework@ico.org.uk; 0303 123 1113
EU / Ireland	Data Protection Commission: dataprotection.ie
Australia	Office of the Australian Information Commissioner: oaic.gov.au
New Zealand	Office of the Privacy Commissioner: privacy.org.nz
Canada	Office of the Privacy Commissioner of Canada: priv.gc.ca
United States	Federal Trade Commission: ftc.gov; and the relevant State Attorney General for children's data under COPPA
South Africa	Information Regulator: inforegulator.org.za

Agreed as between:

Education Institution	3P Learning
Contact name: Email: (if blank, refer to Quote / Subscription)	As set out in our Privacy Policy, these terms are incorporated into your Subscription Agreement when you return the document with your Quote and from the date the licences are assigned to your Education Institution.