					Insert Registered Legal Entity Name Here							
Document number: PII20					Document Title: **Children's Privacy Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Documented information and operational control for child-related processing evidence
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitoring, nonconformity and corrective action for child privacy controls
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.4; Annex A.1.2.5; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Purposes, lawful basis, consent, DPIA and controller records for child-related processing
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Processor contracts and joint-controller responsibilities for child-related processing
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4; Annex A.1.3.5	Controller	Primary	Child-facing obligations, information provision and consent modification or withdrawal
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Objection, access, correction, erasure, request handling and automated decision-making obligations
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Collection, processing, minimization, retention and disposal limits
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Supporting	Disclosure records and disclosure request handling

ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Processor customer agreement, instructions, assistance and records
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Processor support for PII principal obligations and disclosure handling
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protection of records and logging for child-related processing evidence
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Fairness, transparency, purpose limitation, minimization, storage limitation and accountability
GDPR	Article 6; Article 7; Article 8; Article 9	Controller	Primary	Lawfulness, consent conditions, child consent and special-category safeguards
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparent information and child-appropriate notices
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Access, rectification, erasure, restriction, objection and automated decision-making rights
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Controller responsibility, design/default, joint controllers, processors, records, security, DPIA and DPO tasks
ISO/IEC 29100:2020	Clause 5.1; Clause 5.8; Clause 5.9	Both	Primary	Consent and choice, transparency and

				individual participation
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Purpose, collection, minimization, use, retention and disclosure limitation
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Accountability, information security and privacy compliance
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA benefit, threshold determination and preparation for child-related risk assessment
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Consent, purpose, collection, minimization, retention, disclosure and principal participation controls
ISO/IEC TS 27560:2023	Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4	Controller	Supporting	Consent record and receipt structure where consent receipts are used

1. Scope

1.1 This policy defines mandatory privacy requirements for PII processing involving children, child-facing services, services likely to be accessed by children, and processing activities where child PII requires enhanced safeguards.

1.2 This policy applies to:

1.2.1 PII processing activities involving children within the PIMS scope;

1.2.2 child-facing websites, applications, games, educational services, online platforms, connected services, customer portals, learning environments, communities and support channels;

1.2.3 processing where children are directly targeted, likely users, account holders, learners, participants, beneficiaries or represented PII principals;

1.2.4 age assessment, parental responsibility or authorization, child-friendly notices, consent evidence, privacy risk assessment, DPIA triggers, minimization, rights handling, processor restrictions, data sharing and safety-related escalation involving child PII;

1.2.5 controller, joint controller, processor and subprocessor contexts.

1.3 This policy does not replace:

1.3.1 PII03 for processing inventory, lawful basis and ROPA ownership;

1.3.2 PII04 for general privacy notice governance;

1.3.3 PII05 for consent and preference management operation;

1.3.4 PII06 for PII principal rights request workflow;

1.3.5 PII07 for privacy risk assessment and DPIA methodology;

1.3.6 PII08 for privacy by design and default gates;

1.3.7 PII09 for general collection, use, disclosure and sharing controls;

1.3.8 PII10 for retention, deletion and disposal execution;

1.3.9 PII11 for accuracy and quality controls;

1.3.10 PII12 for processor, subprocessor and third-party lifecycle governance;

1.3.11 PII13 for international transfer controls;

1.3.12 PII14 for security and access control;

1.3.13 PII15 for incident and breach handling;

1.3.14 PII18 for monitoring, audit and improvement;

1.3.15 PII21 for AI and automated decision-making privacy controls;

1.3.16 PII22 for marketing privacy and cookies controls.

2. Purpose

2.1 The purpose of this policy is to ensure that child PII is identified, governed, minimized, explained, protected, and evidenced through enhanced privacy safeguards appropriate to child-facing and child-accessible processing.

2.2 This policy supports consistent decision-making for child-related processing without creating a separate child data register, age-assurance register, parental authorization register, safety dashboard, committee or non-canonical evidence object.

3. Objectives

3.1 The objectives of this policy are to:

3.1.1 identify child-facing and child-accessible processing activities in REG02;

3.1.2 define age assessment and parental authorization expectations without prescribing jurisdiction-specific age thresholds inside the policy;

3.1.3 ensure child-friendly privacy notices are maintained in REG07;

3.1.4 ensure consent, parental authorization and withdrawal evidence is maintained in REG05 where applicable;

3.1.5 trigger child-specific privacy risk assessment and DPIA routing through REG04;

3.1.6 ensure rights requests involving children are handled through REG06;

3.1.7 restrict processors, subprocessors and data sharing involving child PII through REG08;

3.1.8 route suspected child PII incidents, misuse, unauthorized access or safety-related PII risks through REG10 and REG12;

3.1.9 maintain audit-ready evidence for child privacy governance through REG12.

4. Policy Statements

4.1 Child-facing processing identification and authorization

4.1.1 [Controller] When a new or materially changed service, feature, campaign, channel or processing activity is proposed, the Process Owner / Business Owner must determine whether the processing is child-facing, likely to be accessed by children, or otherwise involves child PII, and record the determination in REG02.

4.1.2 [Controller] Before collecting age-related information, the Process Owner / Business Owner must define the minimum age-assessment data necessary for the processing purpose and record the method in REG02.

4.1.3 [Controller] Before child PII processing begins, the Process Owner / Business Owner must document the processing purpose, lawful basis, configured child age threshold, parental authorization dependency and evidence location in REG02 and REG05 where consent or authorization is used.

4.1.4 [Joint Controller] Before child PII is processed with a joint controller, the Privacy Lead / PIMS Manager must document child privacy responsibilities, notice responsibility, rights handling, consent or authorization responsibility and escalation responsibility in REG08.

4.1.5 [Processor] Before processing child PII for a customer, the Process Owner / Business Owner must confirm that child-related processing instructions are documented and reflected in REG08.

4.1.6 [Both] Before child PII processing is activated in a system or business process, the Privacy Lead / PIMS Manager must confirm that child-data flags, responsible owners and required evidence objects are recorded in REG02 or REG08 as applicable.

4.2 Child-friendly transparency and notices

4.2.1 [Controller] Before child PII is collected directly from a child or parent, the Process Owner / Business Owner must ensure that a child-appropriate privacy notice is available and recorded in REG07.

4.2.2 [Controller] When a service is designed for children or is likely to be accessed by children, the Process Owner / Business Owner must provide layered notice content that separates child-appropriate explanations from parent or guardian information and record the notice version in REG07.

4.2.3 [Controller] When child PII is collected indirectly, the Process Owner / Business Owner must document the source, notice approach and timing of notice provision in REG02 and REG07.

4.2.4 [Controller] When a child-facing processing purpose, data category, recipient category, retention reference, consent mechanism or rights route changes, the Privacy Lead / PIMS Manager must review and update the relevant notice record in REG07 before the change is implemented.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Exceptions

9.1 [All] Before deviating from a child privacy requirement in this policy, the requesting Process Owner / Business Owner must submit an exception rationale and compensating control evidence in REG12.

9.2 [Conditional] When an exception affects child consent, parental authorization, child-facing notice, profiling, automated decision-making, DPIA outcome, disclosure or safety-related processing, the Data Protection Officer / Privacy Advisor must review the exception and record advice in REG04 or REG12.

9.3 [Conditional] When an exception creates or preserves high residual risk for child PII, Top Management must approve or reject the exception and record the decision in REG04 and REG12.

9.4 [All] Before an approved child privacy exception expires, the Privacy Lead / PIMS Manager must review closure, renewal or corrective action status and record the outcome in REG12.

10. Enforcement

10.1 [All] When noncompliance with this policy is identified, the Privacy Lead / PIMS Manager must record the nonconformity and corrective action in REG12.

10.2 [Both] When unauthorized child PII processing, disclosure, access or use is suspected, the Incident Response Coordinator must initiate incident escalation and record evidence in REG10 and REG12.

10.3 [Both] When a processor, subprocessor, supplier or data-sharing recipient fails to meet child-related privacy obligations, the Vendor / Procurement Owner must record remediation, escalation or termination action in REG08 and REG12.

10.4 [All] When repeated or systemic child privacy nonconformities occur, Top Management must review the issue and record the management action in REG12.

11. Review and Maintenance

11.1 [All] At least annually, the Privacy Lead / PIMS Manager must review this policy for continued suitability and record the review outcome in REG12.

11.2 [Conditional] When laws, services, technologies, age-assessment methods, consent mechanisms, child-facing user journeys or processing risks materially change, the Privacy Lead / PIMS Manager must review affected child privacy controls and record the outcome in REG02, REG04 or REG12.

11.3 [Controller] At least annually and after material interface changes, the Process Owner / Business Owner must review child-facing notice and consent content and record the review in REG05 and REG07.

11.4 [All] After child privacy corrective actions are closed, the Internal Audit / Compliance Reviewer must verify effectiveness and record verification evidence in REG12.

12. Related Policies

12.1 PII01 - Privacy Information Management System Policy

12.2 PII02 - Privacy Roles, Responsibilities and Accountability Policy

12.3 PII03 - PII Processing Inventory and Lawful Basis Policy

12.4 PII04 - Privacy Notice and Transparency Policy

12.5 PII05 - Consent and Preference Management Policy

12.6 PII06 - PII Principal Rights Management Policy

12.7 PII07 - Privacy Risk Assessment and DPIA Policy

12.8 PII08 - Privacy by Design and Default Policy

12.9 PII09 - PII Collection, Use, Disclosure and Sharing Policy

12.10 PII10 - PII Retention, Deletion and Disposal Policy

12.11 PII11 - PII Accuracy and Quality Policy

12.12 PII12 - Processor, Subprocessor and Third-Party Privacy Management Policy

12.13 PII13 - International PII Transfer Policy

12.14 PII14 - PII Security and Access Control Policy

12.15 PII15 - PII Incident and Breach Management Policy

12.16 PII17 - PIMS Documented Information and Evidence Management Policy

12.17 PII18 - PIMS Monitoring, Audit and Improvement Policy

12.18 PII21 - AI and Automated Decision-Making Privacy Policy

12.19 PII22 - Marketing Privacy and Cookies Policy

13. Reference Standards and Frameworks

13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].

13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].

13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.4; Annex A.1.2.5; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.3.1; 4.3.2; 4.3.5; 4.6.1; 4.8.1; 7.1; 7.2; 7.4].

13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.3; 4.7.4; 5.7; 6.3; 7.7].

13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4; Annex A.1.3.5. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.3; 7.3; 11.3].

13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.3; 4.6.5; 7.6].

13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9. Addressed by clauses [4.1.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 7.1].

13.8 ISO/IEC 27701:2025 - Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.1; 4.7.2; 4.8.1; 7.7].

13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.5.4; 4.7.3; 4.7.4; 5.7; 6.3; 7.7].

13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 7.7].

13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.6.2; 4.6.4; 4.8.1; 7.5; 7.8; 10.2].

13.12 GDPR - Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2). Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.4; 4.4.5; 4.8.1; 8.1].

13.13 GDPR - Article 6; Article 7; Article 8; Article 9. Addressed by clauses [4.1.3; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.4.3; 7.4; 11.3].

13.14 GDPR - Article 12; Article 13; Article 14. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.3; 11.3].

13.15 GDPR - Article 15; Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.3; 4.6.5; 7.6].

13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.6.1; 4.6.2; 4.7.3; 4.8.2; 5.3; 6.4; 7.2; 9.2].

13.17 ISO/IEC 29100:2020 - Clause 5.1; Clause 5.8; Clause 5.9. Addressed by clauses [4.2.1; 4.2.2; 4.3.1; 4.3.3; 4.5.1; 4.5.2; 4.5.3].

13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 4.4.4; 4.4.5; 4.7.1].

13.19 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.6.2; 4.6.4; 4.8.1; 4.8.2; 6.1; 8.5; 10.1].

13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.4.3; 4.6.1; 4.6.3; 6.4; 7.2; 9.2].

13.21 ISO/IEC 29151:2022 - Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 4.5.2; 4.7.1; 7.4].

13.22 ISO/IEC TS 27560:2023 - Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4. Addressed by clauses [4.3.2; 4.3.4; 4.3.5; 7.4].