SOFTWARE PROCUREMENT

Section: Human Resources / Foundations	**Effective Date:** September 2026
Legal Cross-References: The Freedom of Information and Protection of Privacy Act (FIPPA); The Personal Health Information Act (PHIA); Manitoba Education – Literacy with ICT Across the Curriculum	**Administrative Procedures Cross-Reference:** AP 234 Responsible Use of Information and Communication Technologies (ICT); AP 506 Purchasing Authority; AP 118 Selection of Materials; AP 203 Digital Citizenship

1. Purpose and Philosophy

The Swan Valley School Division (SVSD) supports the effective and innovative use of digital tools, applications, software, and online cloud services to enhance student learning, optimize organizational communication, and foster operational excellence. Access to digital technologies is a vital asset for modern instruction and administrative functioning.

The purpose of Administrative Procedure 509 is to establish a rigorous, standardized, and division-wide process for the evaluation, approval, procurement, deployment, management, and decommissioning of all software, web-based applications, mobile apps, digital learning tools, and artificial intelligence (AI) platforms utilized across the Division.

Specifically, this procedure is established to:

- **Protect Personal Privacy:** Safeguard personal information and personal health information of students, parents, staff, and community members in compliance with Manitoba and federal legislation.
- **Ensure Legislative Compliance:** Fulfill all statutory obligations under The Freedom of Information and Protection of Privacy Act (FIPPA) and The Personal Health Information Act (PHIA).
- **Enhance Cybersecurity:** Assess and mitigate technical vulnerabilities, data breach risks, unauthorized data access, and unverified third-party vendor practices.
- **Promote Responsible Stewardship:** Ensure financial efficiency, avoid unnecessary duplication of software functionality, and align digital procurements with divisional priorities.
- **Ensure Accessibility and Equity:** Guarantee that selected digital resources accommodate diverse learning needs and support inclusive educational practices.

2. Definitions

- **Digital Tool / Software:** Any software application, mobile app, cloud-based platform, web service, digital learning tool, browser extension, digital content platform, or artificial intelligence (AI) solution utilized for instructional, administrative, or operational purposes within the Division.
- **Personal Information (PI):** Recorded information about an identifiable individual as defined under FIPPA, including but not limited to an individual's name, home address, email address, student identification number, age, gender, educational history, or grades.

- **Personal Health Information (PHIA):** Recorded information about an identifiable individual that relates to the individual's physical or mental health, health care history, medical diagnosis, or disability as defined under PHIA.
- **Privacy Impact Assessment (PIA):** A structured process and evaluation tool used to identify, analyze, and mitigate potential privacy risks associated with new or modified digital tools, systems, or data collection practices.
- **Data Residency / Cross-Border Data Transfer:** The physical or geographical location where data (including server backups and replication) is hosted, stored, or processed by a vendor or its subcontractors.
- **Vendor:** Any third-party provider, developer, distributor, or organization supplying digital tools, software, platforms, or related technology services to the Division.

3. General Principles

All digital tools considered or implemented within Swan Valley School Division must adhere to the following core principles:

- **Strategic & Educational Alignment:** Digital tools must directly support identified curriculum standards, instructional goals, operational requirements, or administrative efficiencies.
- **Data Minimization:** Digital tools shall collect and store only the minimum personal information strictly required to fulfill the intended educational or business function.
- **Safeguarding & Data Ownership:** All student and staff data remains the sole property of the Swan Valley School Division. Data must be protected against unauthorized access, disclosure, monetization, or commercial profiling.
- **Canadian Data Residency Preference:** To ensure optimal privacy governance and minimize jurisdictional legal risks, preference is given to software solution providers that store and back up data within Canadian servers. Secondary preference will be given to vendors that store data in the United States of America, but have the primary or backup data stored within Canada.
- **Accessibility and Inclusion:** Software tools must comply with recognized accessibility standards, such as the Web Content Accessibility Guidelines (WCAG), to ensure equitable access and usability for all users. Digital tools must support the diverse learning, communication, and accessibility needs of students, staff, families, and community members, enabling all individuals to fully participate and effectively perform their roles within the organization.
- **Fiscal Stewardship:** Digital procurements must adhere to financial approval limits, represent sound value for money, and avoid duplication of existing Division-vetted platforms.

4. Procedures & Vetting Framework

4.1 Approval Requirement

No employee, department, or school shall purchase, install, download, subscribe to, create accounts for, or deploy any software or digital tool that collects, stores, transmits, or processes

student or staff information without obtaining formal authorization through the Division's software vetting process.

This requirement applies universally, regardless of whether the software is free, trial-based, freemium, funded via school-generated funds, acquired through grant funding, or purchased with divisional budgets.

4.2 Request for Review Submission

Staff members seeking to introduce a new digital tool must submit a formal Request for Software Review (i.e. Part 1 of Appendix A – Privacy Impact Assessment (PIA) Tool) to the Network Administrator. The submission must be submitted and approved via Steps 2 and 3 of the PIA prior to procurement or implementation.

4.3 Educational and Operational Review

The request shall be reviewed and signed off by the Principal or Department Supervisor to verify:

- **Priority Alignment:** Direct connection to divisional learning goals or operational priorities.
- **Existing Solutions Check:** Confirmation with IT Services that an existing, approved application cannot fulfill the required function.
- **Equity & Accessibility:** Evaluation of user accessibility, interface usability, and student inclusion capabilities.

4.4 Security & Technical Review

The Network Administrator shall conduct a technical security analysis examining:

- **Authentication & Access:** Compatibility with Divisional Single Sign-On (SSO) if installed on our servers and support for Multi-Factor Authentication (MFA).
- **Encryption Standards:** Enforcement of industry-standard encryption protocols both in transit and at rest.
- **Network & System Compatibility:** Bandwidth requirements, device operating system support, and infrastructure impact.
- **Third-Party Certifications & Audits:** Review of vendor reports, certifications, or third-party penetration test summaries as per industry standards.

4.5 Legal and Contractual Review

Where vendor agreements, Terms of Service (ToS), or Data Processing Agreements (DPAs) are required, the Division shall ensure terms include:

Divisional Data Ownership: Unambiguous affirmation that SVSD retains sole ownership of all uploaded data, pupil work, and user logs.

- **Breach Notification:** Mandatory prompt written notification to SVSD (within 24 to 48 hours) in the event of any actual or suspected security incident or data breach.
- **Subprocessor Disclosure:** Full disclosure of all third-party subprocessors utilized by the vendor and commitment to maintain equivalent privacy safeguards.

4.6 Privacy & Data Residency Review (FIPPA / PHIA)

The Divisional Privacy Officer (Secretary Treasurer) shall conduct a privacy impact assessment on proposed software solutions to ensure compliance with FIPPA and PHIA:

- **Data Collection & Monetization:** Confirmation that the vendor does not sell, monetize, profile, or display targeted advertising based on student or staff data.
- **Data Residency Assessment:** Verification of server location and backup protocols. Vendors host data in Canada wherever feasible. If US or foreign hosting is required, a risk analysis is conducted regarding foreign lawful access and contractual protections.
- **Consent & Notification:** Determination of whether parent/guardian notification or explicit consent forms are mandated prior to student account creation.
- **Data Retention & Destruction:** Verification that vendor terms mandate secure data deletion upon contract termination or account inactivation.

4.7 Approval Decisions & Status

Following multi-disciplinary evaluation, proposed digital tools shall receive one of four formal approval designations:

Approval Designation	Definition and Operational Scope
APPROVED	Authorized for division-wide deployment and standard classroom or administrative use subject to standard guidelines.
APPROVED WITH CONDITIONS	Authorized for use under specific restrictions (e.g., parent consent required, limited data fields, restricted grade levels, or Canadian storage).
PILOT APPROVAL	Authorized for limited time-bound testing by a designated classroom or department prior to division-wide consideration.
NOT APPROVED	Prohibited for use. Software presents unacceptable privacy risks, cybersecurity vulnerabilities, legal concerns, or unnecessary financial cost.

The Superintendent of Schools shall have final decision-making authority on software approval decisions if the Secretary-Treasurer's approval decision is appealed.

4.8 Artificial Intelligence (AI) Tools & Generative Services

Emerging artificial intelligence (AI) tools, large language models (LLMs), and automated content generation software require heightened privacy and security scrutiny. In addition to standard vetting, AI digital tools must satisfy specific safeguards:

- **Prohibition on Personal Information/Personal Health Information Entry:** Staff and students are strictly prohibited from entering identifiable student or staff personal information or personal health information into unvetted or public generative AI tools.

- **Model Training Rights:** Vetting must confirm that the AI vendor does not utilize uploaded divisional content, student prompts, or intellectual property to train public AI models.
- **Algorithmic Bias & Accuracy:** Evaluations must consider potential algorithmic bias, output hallucination risks, and age-appropriateness.

5. Roles and Responsibilities

- **Superintendent:** If appealed, provides executive oversight and serves as final authority for approval decisions.
- **Network Administrator:** Manages the software vetting workflow, conducts security evaluations, maintains the Division Approved Software Catalog, and manages technical deployment.
- **Secretary-Treasurer/Privacy Officer:** Reviews Privacy Impact Assessments (PIAs), evaluates FIPPA/PHIA compliance, assesses financial implications and determines parent consent requirements.
- **Principals & Department Supervisors:** Ensure staff within their school or department adhere strictly to approved software lists and submit PIA forms for new tool requests.
- **Instructional & Administrative Staff:** Utilize only division-approved software, maintain password security, report unvetted applications, and ensure student compliance.

6. Compliance and Consequences for Misuse

Compliance with this administrative procedure is mandatory for all Swan Valley School Division employees. Installing, purchasing, or utilizing unvetted software platforms exposes student personal information to unauthorized third parties and creates significant legal and cybersecurity risks for the Division.

Consistent with the enforcement provisions of AP 234 Responsible Use of Information and Communication Technologies, violations of this administrative procedure by staff may result in:

- **Access Restrictions:** Immediate suspension or permanent removal of access to divisional networks, administrative accounts, and computing devices.
- **Disciplinary Action:** Progressive disciplinary action up to and including formal written reprimand, suspension, or recommendation for termination of employment.
- **Statutory / Legal Remedies:** Legal action or referral to law enforcement authorities where unauthorized software usage leads to illegal acts or severe privacy breaches under Manitoba law.

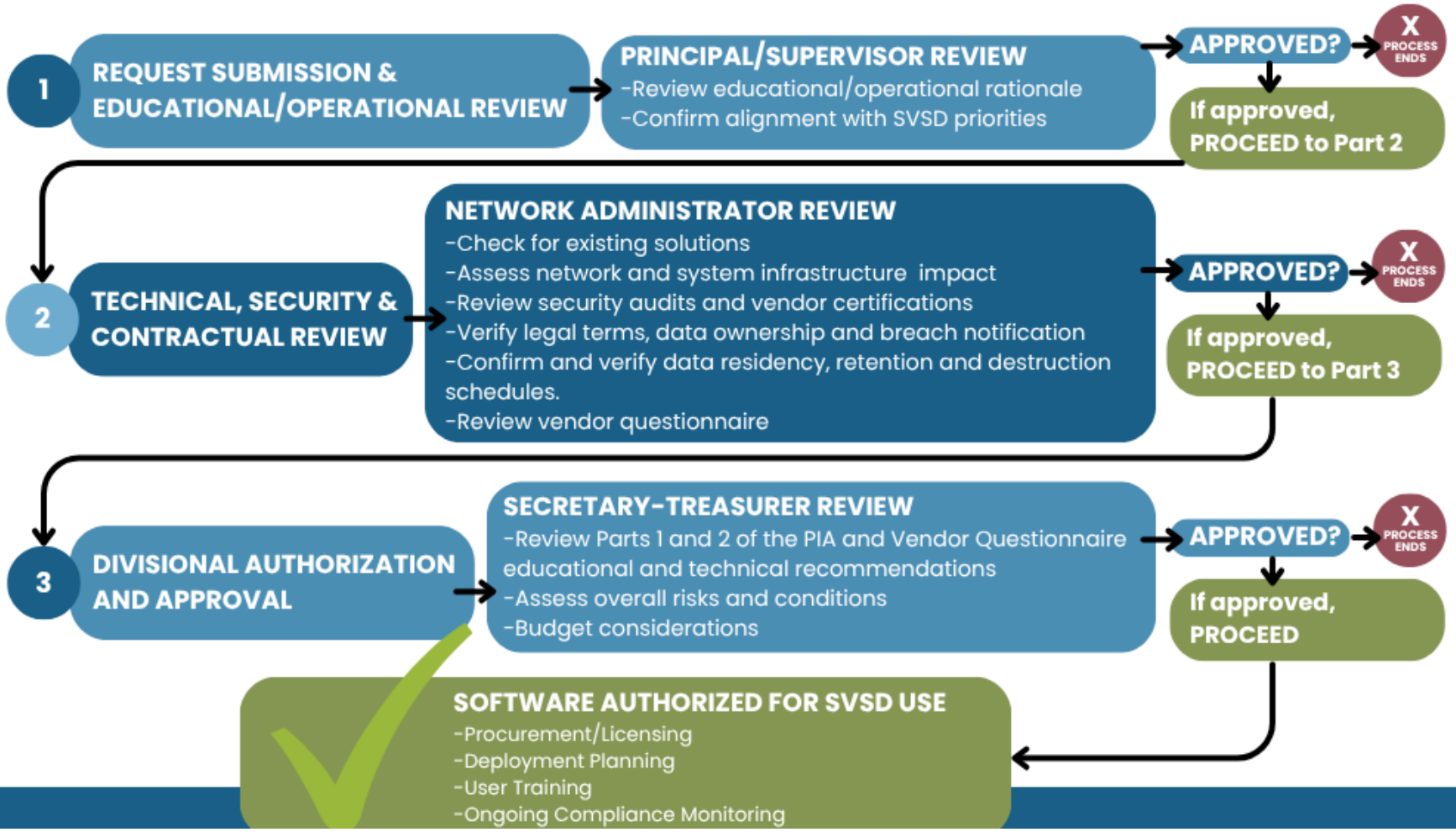
Swan Valley School Division

AP509 Software Procurement - Appendix A

PRIVACY IMPACT ASSESSMENT (PIA) & SOFTWARE VETTING TOOL

A standardized decision-making framework to evaluate and address potential privacy, technical, and legal risks when introducing new software, digital tools, or online services.

REQUEST SUBMISSION - Requester and Principal complete Part 1
Provide project details, vendor information, purpose, data collected, and complete educational/operational review.



SVSD PRIVACY IMPACT ASSESSMENT (PIA) & SOFTWARE VETTING TOOL

Preamble & Purpose: The Privacy Impact Assessment (PIA) is a standardized decision-making framework used to evaluate and address potential privacy, technical, and legal risks when introducing new software applications, cloud platforms, digital tools, or online services in Swan Valley School Division. This three-part tool ensures full compliance with FIPPA, PHIA, and SVSD Administrative Procedure 509 Software Procurement.

PART 1: REQUEST SUBMISSION & EDUCATIONAL / OPERATIONAL REVIEW

Field Category	Requester & Educational Evaluation Details
Project/Software Name: *Exact application name, version, and official vendor URL*	
Application Date:	
Department/School/Grade: *School name, grade levels, or operational unit*	
Project Lead/Requester: *Name and role submitting staff member*	
Vendor/External Partner: *Company name, primary contact details, and platform hosting details*	
Product Specification & Target Users: *Describe the target audience (students, teachers, parents, admin) and software platform (Web, iOS, Android, Windows).*	
Instructional / Business Rationale & Purpose: *Detail the educational purpose or operational efficiency gained. Explain key learning goals or administrative workflows.*	
Existing Solutions & Equity Check: *Confirm that existing divisional tools cannot fulfill this function. Outline accessibility features.*	
Parent Notification & Consent Requirements: *Determine if formal parent/guardian notification or signed consent forms are legally mandated prior to student account creation.*	

PART 1: PRINCIPAL / SUPERVISOR SIGN-OFF & AUTHORIZATION

Principal/Department Supervisor Name:

Date:

Approval Status:

☐ APPROVED
☐ APPROVED WITH CONDITIONS
☐ PILOT APPROVAL
☐ NOT APPROVED

Status Details / Specific Conditions:

Authorized Signature: X _____

PART 2: TECHNICAL, SECURITY & CONTRACTUAL REVIEW

Technical Verification Category	Network Administrator Evaluation & Safeguards
Existing Solutions Check & Duplication Audit: *IT Services confirmation whether an approved application currently licensed by SVSD provides equivalent functionality.*	
Network & System Infrastructure Impact: *Assess bandwidth consumption, firewall/port requirements, OS compatibility, and device deployment protocols.*	
Security Audits & Vendor Certifications: *Evaluate vendor reports, certifications, or third-party penetration testing summaries to industry standards.*	
Legal Terms & Contractual Safeguards: *Verify Terms of Service (ToS): (a) 100% SVSD data ownership, (b) mandatory 24-48 hour breach notification, and (c) full disclosure of sub-processors.*	
Data Residency & Server Location Assessment: *Identify primary and backup server locations. Confirm Canadian data residency preference or evaluate cross-border legal access risks outside of Canada..*	
Artificial Intelligence (AI) Safeguards Check: *Confirm vendor does not use SVSD prompts or student data to train public AI models. Re-verify absolute prohibition on entering Personal Information/Personal Health Information into AI tools.*	
Data Collection & Monetization Restrictions: *Verify that vendor agreement prohibits selling, monetizing, profiling, or targeted advertising using student or staff personal data under FIPPA/PHIA.*	

PART 2: NETWORK ADMINISTRATOR SIGN-OFF & TECHNICAL RECOMMENDATION

Network Administrator Name:

Date:

Approval Status:

☐ APPROVED

☐ APPROVED WITH CONDITIONS

☐ PILOT APPROVAL

☐ NOT APPROVED

Status Details / Specific Conditions:

Authorized Signature: X _____

PART 3: SECRETARY-TREASURER FINAL REVIEW

PART 3: SECRETARY-TREASURER / PRIVACY OFFICER AUTHORIZATION & FINAL REVIEW	
Secretary-Treasurer / Privacy Officer Name:	**Date:**
Approval Status: ☐ APPROVED ☐ APPROVED WITH CONDITIONS ☐ PILOT APPROVAL ☐ NOT APPROVED	**Status Details / Specific Conditions:**
Authorized Signature:	**X** _____

Vendor Privacy, Security & Educational Information Questionnaire

Supporting Documentation for Privacy Impact Assessment (PIA) - Part 1. Can be emailed to vendors by principals to support the completion of Step 1 of the PIA.

Purpose: This questionnaire is to be completed by the software vendor to assist Swan Valley School Division (SVSD) in evaluating new software applications, cloud services, educational technologies, and digital tools. Completion of this form does not constitute approval or procurement.

SECTION A: Vendor & Product Information

1. Product Information	
Product Name:	
Current Version Number:	
Official Product Website URL:	
Date Submitted:	

2. Vendor Information	
Company Name:	
Head Office Address:	
Primary Contact Name and Title:	
Email Address:	
Telephone Number:	
Technical Support Contact Information:	

3. Hosting Information

Where is the application hosted?

☐ Vendor-hosted SaaS ☐ Private Cloud ☐ Other: _____
☐ Public Cloud Service ☐ On-Premise

Hosting Provider(s):	
Primary Data Centre Location(s):	
Backup Data Centre Location(s)	

SECTION B: Product Description & Intended Use

4. Product Review	
Please provide a brief description of the software/service:	

5. Intended Users (Check all that apply)

☐ Students ☐ Educational Assistants ☐ Other: _____
☐ Teachers ☐ School Administrators
☐ Division Office Staff ☐ Parents/Guardians

6. Supported Platforms (Check all that apply)

☐ Web Browser ☐ MacOS ☐ Other: _____
☐ Windows ☐ iOS
☐ Android ☐ Chromebook

7. Educational or Operational Benefits

Describe the educational outcomes, learning objectives, productivity gains, or operational efficiencies your product provides.	

SECTION C: Data Collection & Privacy

8. Personal Information Collected

Please identify all information your product may collect, store, process, or transmit.

DATE ELEMENT	REQUIRED?	OPTIONAL?
Full Name	☐	☐
Email Address	☐	☐
Health Information	☐	☐
Student Number	☐	☐
Date of Birth	☐	☐
Grade Level	☐	☐
Attendance Data	☐	☐
Academic Records	☐	☐
Assignments/Work Samples	☐	☐
Assessment Results	☐	☐
Student Specification Plan Information	☐	☐
IP Address	☐	☐
Device Information	☐	☐
Location Date	☐	☐
Photos	☐	☐
Videos	☐	☐
Audio Recordings	☐	☐
Other	☐	☐

Please describe any additional data collected:	

9. Purpose of Collection	
For each type of personal information collected, explain why it is necessary.	

10. Retention, Archiving & Destruction Schedule:	
Confirm contractual timeline and internal/external protocol for secure data deletion/destruction upon account inactivation or contract termination.	

11. Student Information Protection

Does the product collect more personal information than is required to deliver the service?

☐ Yes ☐ No

If yes, explain:	

SECTION D: Accessibility & Equity

12. Accessibility Features

Please identify accessibility features available within the product.

☐ Screen Reader Compatibility
☐ Keyboard Navigation
☐ Closed Captioning
☐ Adjustable Font Size
☐ Text-to-Speech
☐ Speech-to-Text
☐ Colour Contrast Controls
☐ Adjustable Font Sizes
☐ Language Translation Features
☐ WCAG 2.1 AA Compliance
☐ Other Accessibility Features

Please describe:	

13. Accessibility Compliance

Has the product been independently tested for accessibility compliance?

☐ Yes ☐ No

If yes, provide details and supporting documentation:	

SECTION E: Authentication & Security

14. User Authentication

Authentication Method	Supported	
Microsoft Entra ID (Azure AD)	☐ Yes ☐ No	Other: _____
SVSD Federation	☐ Yes ☐ No	
OAuth 2.0	☐ Yes ☐ No	
Google Federation	☐ Yes ☐ No	
Multi-Factor Authentication (MFA)	☐ Yes ☐ No	

15. Encryption

Security Controls	Supported	
TLS 1.2 or higher for data in transit	☐ Yes ☐ No	Other: _____
Data encrypted at rest	☐ Yes ☐ No	
AES-256 encryption at rest	☐ Yes ☐ No	
Regular security updates	☐ Yes ☐ No	
Vulnerability management program	☐ Yes ☐ No	

16. Security Certifications

Please indicate all certifications held:

☐ SOC 2 Type II ☐ CSA STAR ☐ Independent Penetration Testing
☐ ISO 27001 ☐ Cyber Essentials ☐ Other: _____

Please attach current certifications where available.

SECTION F: Data Usage & Legal Compliance

17. Data Ownership

Please confirm:

☐ SVSD retains ownership of all data entered into the system.
☐ Vendor claims no ownership rights over customer data.

18. Advertising & Monetization

Please confirm the following:

Personal information is not sold to third parties	☐ Yes	☐ No
Personal information is not used for targeted advertising	☐ Yes	☐ No
Personal information is not used for profiling users	☐ Yes	☐ No
Student data is not monetized	☐ Yes	☐ No
Staff data is not monetized	☐ Yes	☐ No

19. Third-Party Data Sharing

Does the product share personal information with subcontractors, service providers, or sub-processors?

☐ Yes ☐ No

If yes, identify all third parties and their jurisdiction(s):

SECTION G: Parent Consent Requirements

20. Consent Requirements

Based on your organization's understanding of educational sector requirements, does your service require:

☐ Parent/Guardian Notification
☐ Parent/Guardian Consent
☐ No Additional Consent Required

Please explain:

SECTION H: Artificial Intelligence (AI) Safeguards

21. Artificial Intelligence Features

Does your product include any Artificial Intelligence functionality?

☐ Yes ☐ No

If yes, describe the AI functions:

22. AI Training Practices

Please confirm the following:

Customer data is not used to train public AI models	☐ Yes	☐ No
Student data is not used to train AI models	☐ Yes	☐ No
Staff data is not used to train AI models	☐ Yes	☐ No
Customer data can be excluded from AI training	☐ Yes	☐ No
AI features can be disabled by administrators	☐ Yes	☐ No

23. AI Data Protection

Describe safeguards used to prevent the use of personal information or personal health information within AI systems.

SECTION I: Vendor Declaration

I certify that the information provided in this questionnaire is complete and accurate to the best of my knowledge and that supporting documentation can be provided upon request.

Vendor Representative Name and Title:	
Company:	
Signature:	
Date:	

Required Supporting Documentation

Please attach the following where available:

☐ Privacy Policy
☐ Terms of Service
☐ Data Processing Agreement (DPA)
☐ Vendor reports, certificates, or 3rd party penetration test summaries.
☐ Accessibility Conformance Report
☐ Security Whitepaper
☐ Data Retention and Destruction Policy
☐ List of Sub-Processors
☐ AI Governance Statement
☐ Other Supporting Documentation: _____