

Specimen — illustrative example

Riverstem Learning is a fictional organisation. This document comes from the scenario described on riskwoven.com/examples, and is not an assessment of any real entity. It is advisory output to support your own decisions: not legal advice, not a certification, and not an audit.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.

Privacy Breach Response Procedure

Riverstem Learning

Document type	procedure	Version	1.0 Draft
Owner	Director of Learning	Customer decision role	Chief Executive Officer
Effective date	Upon customer release	Review cycle	Annual
Framework basis	RiskWoven AI practical best practices		
Jurisdiction	Ontario, Canada		
Prepared for	Riverstem Learning	Industry	Education
Organization size	26-100	Locations	Not specified

Advisory draft for accountable-owner and professional review. Validate legal, regulatory, contractual, technical and operational requirements before customer release. This is not legal advice, a certification, or a compliance determination.

1. Purpose

This procedure sets out the steps Riverstem Learning follows when a privacy breach is suspected or confirmed. It covers containment, assessment, notification decisions and

documentation. The procedure applies whether or not notification is ultimately required.

2. Scope

This procedure applies to any event involving personal information held by Riverstem Learning, including information about learners, guardians, partner school staff and Riverstem employees. It covers information processed in Google Cloud Montreal region, Google Workspace for Education and any other system holding personal information on Riverstem's behalf.

The procedure applies to all Riverstem staff, contractors and third-party processors acting under Riverstem's instruction.

3. Definitions

Privacy breach: The loss of, unauthorised access to, or unauthorised disclosure of personal information, whether accidental or deliberate. This includes theft, loss of a device containing personal information, unauthorised viewing, and transmission to an unintended recipient.

Real risk of significant harm: A breach creates a real risk of significant harm when the sensitivity of the information and the probability that it will be misused are such that an affected individual could experience injury. Harm includes identity theft, financial loss, damage to reputation, humiliation, and physical harm. For learners, harm also includes interference with education and safeguarding risk.

Affected individual: A person whose personal information is involved in the breach. For Riverstem this may be a learner, a guardian, a partner school staff member or a Riverstem employee.

Regulator: The privacy commissioner or other supervisory authority with jurisdiction over the breach. For breaches involving Ontario residents, this may be the Information and Privacy Commissioner of Ontario or, where applicable federal law applies, the Office of the Privacy Commissioner of Canada. The applicable statute has not been confirmed for Riverstem; the Privacy Officer confirms the applicable regulator for each breach and Riverstem must obtain independent legal review to determine which statute governs its operations.

4. Roles and Responsibilities

Privacy Officer: Leads the breach assessment, determines whether notification is required, drafts regulator and affected-individual notifications, and maintains the breach register.

IT Manager (Incident Lead): Leads technical containment and evidence preservation. Coordinates with the Privacy Officer on scope and affected systems.

Chief Executive Officer: Makes the final notification decision where the Privacy Officer's assessment recommends notification or where the decision is contested. Receives all Critical-severity breach reports.

Designated Safeguarding Lead: Consulted immediately when a breach involves safeguarding notes or may affect learner safety. Determines whether safeguarding authorities must be notified.

Director of Learning (Document Owner): Leads communication with guardians and partner schools once a notification decision is made. Reviews this procedure annually.

All staff: Report suspected breaches immediately to the Privacy Officer or IT Manager.

5. Procedure

This procedure has five stages: Detection and Initial Report, Containment and Evidence Preservation, Assessment, Notification Decision and Execution, and Documentation and Lessons Learned.

6. 5.1 Detection and Initial Report

Step 1. Any staff member who suspects a privacy breach reports it immediately to the Privacy Officer or IT Manager by the fastest available channel. The report includes what happened, when it was discovered, what information may be involved, and who may be affected.

Step 2. The Privacy Officer or IT Manager acknowledges the report within 30 minutes for any breach that may be Critical severity. For other severities, acknowledgement occurs within the same business day.

Step 3. The Privacy Officer opens a breach record in the breach register, assigning a unique identifier and recording the date, time, reporter and initial description.

7. 5.2 Containment and Evidence Preservation

Step 4. The IT Manager takes immediate action to stop the breach from continuing. Actions may include revoking access, isolating affected systems, disabling compromised accounts, or retrieving devices. The IT Manager records each action and its time in the breach record.

Step 5. The IT Manager preserves evidence before any remediation that would alter it. Evidence includes access logs, audit trails, email headers and screenshots. Evidence is stored in a restricted location accessible only to the incident team.

Step 6. The IT Manager limits access to affected information during the investigation. Only personnel required for containment and assessment view the affected records. Viewing is logged.

Step 7. If the breach involves a third-party processor, the IT Manager contacts the processor immediately to confirm containment on their systems and to request relevant logs.

8. 5.3 Assessment

Step 8. The Privacy Officer identifies the scope of the breach:

- What personal information is involved (identity, contact details, submitted work, assessment records, safeguarding notes).
- How many individuals are affected and in which categories (learners, guardians, partner school staff, employees).
- Which systems and storage locations are involved.
- Whether the information has left Riverstem's control and, if so, to whom.

Step 9. The Privacy Officer assesses sensitivity. Safeguarding notes are the most restricted category. Assessment records and submitted work are sensitive where they could identify a learner's performance or circumstances. Identity and contact details are sensitive where they could enable contact with a minor.

Step 10. The Privacy Officer assesses the probability of misuse. Factors include whether the recipient is known, whether the information was encrypted, whether it has been recovered, and whether there is evidence of malicious intent.

Step 11. The Privacy Officer determines whether the breach creates a real risk of significant harm to any affected individual. The assessment is documented in the breach record with the

reasoning for the conclusion.

Step 12. If the breach involves safeguarding notes or may affect learner safety, the Privacy Officer consults the Designated Safeguarding Lead before completing the assessment. The Designated Safeguarding Lead determines whether safeguarding authorities must be notified and records that determination.

Step 13. The Privacy Officer identifies the applicable regulator and any statutory notification deadline. The Privacy Officer records the basis for this determination. Where the applicable law is uncertain, the Privacy Officer escalates to external privacy counsel for independent review before the notification decision.

9. 5.4 Notification Decision and Execution

Step 14. The Privacy Officer prepares a written recommendation stating whether notification to the regulator and to affected individuals is required, and the reasoning. The recommendation includes draft notification content.

Step 15. The Chief Executive Officer reviews the recommendation and makes the notification decision. The decision and its reasoning are recorded in the breach record. If the Chief Executive Officer is unavailable, the Director of Learning may make the decision for breaches assessed as High severity or below; Critical-severity decisions require the Chief Executive Officer.

Step 16. If notification to the regulator is required, the Privacy Officer submits the notification within the deadline set by applicable law. The applicable statutory deadline must be confirmed by Riverstem through independent legal review before this procedure is relied upon; the Privacy Officer confirms the deadline for each breach in the interim. The Privacy Officer retains a copy of the submission and any acknowledgement.

Step 17. If notification to affected individuals is required, the Director of Learning coordinates delivery. For learners, notification is sent to the guardian and, where the partner school agreement requires, to the partner school for onward communication. Notification includes:

- A description of the breach.
- The types of personal information involved.
- Steps Riverstem has taken to contain the breach.
- Steps the individual can take to reduce risk of harm.
- Contact information for questions.

Step 18. The Director of Learning notifies affected partner schools of any breach involving their learners, regardless of whether individual notification is required, unless doing so would compromise an ongoing investigation. The timing and content are agreed with the Privacy Officer.

Step 19. If notification is not required, the Privacy Officer records the reasoning in the breach record. The record is retained for the period set in the Records Retention and Disposal Policy.

10. 5.5 Documentation and Lessons Learned

Step 20. The Privacy Officer completes the breach record within a period set by Riverstem Learning; 30 calendar days from breach closure is offered as a starting point and is not derived from a statutory requirement. The record includes:

- Breach identifier, dates of discovery and closure.
- Description of the breach and root cause.
- Personal information and individuals affected.
- Containment and remediation actions.
- Assessment of harm and reasoning.
- Notification decision, reasoning and evidence of delivery.
- Corrective actions to prevent recurrence.

Step 21. The Privacy Officer convenes a lessons-learned review for any Critical-severity breach and for any breach that required notification. The review includes the IT Manager, the Director of Learning and any other staff involved in the response.

Step 22. The lessons-learned review identifies control failures, procedural gaps and improvement actions. The Privacy Officer records the findings and assigns owners and target dates for each action.

Step 23. The Privacy Officer reports corrective actions to the Chief Executive Officer and tracks them to completion. Overdue actions are escalated to the Chief Executive Officer.

Step 24. The Privacy Officer updates this procedure, the Privacy and Personal Information Policy or related controls where the lessons-learned review identifies a gap.

11. Escalation

Any breach involving safeguarding notes is escalated immediately to the Designated Safeguarding Lead and the Chief Executive Officer.

Any breach assessed as Critical severity is escalated to the Chief Executive Officer within 30 minutes of acknowledgement; this target is Riverstem Learning's own parameter and 30 minutes is offered as a recommended starting point for the organisation to confirm.

Any breach where the Privacy Officer and IT Manager disagree on scope, severity or notification is escalated to the Chief Executive Officer for decision.

Any breach involving a third-party processor that does not cooperate with containment or evidence requests is escalated to the Chief Executive Officer and, where the contract permits, to external privacy counsel.

12. Metrics

The Privacy Officer reports the following metrics to the Chief Executive Officer on a cycle set by Riverstem Learning; quarterly is offered as a starting point:

- Number of breaches reported and assessed.
- Percentage of breach assessments completed within the target period.
- Percentage of notification decisions documented before the applicable deadline.
- Percentage of required regulator and individual notifications delivered on time.
- Number of corrective actions arising from lessons-learned reviews.
- Number of corrective actions overdue.
- Number of reviewed exceptions to this procedure past their expiry date.

13. Related Documents

- Privacy and Personal Information Policy
- Security Incident Response Procedure
- AI Incident Response Procedure
- Records Retention and Disposal Policy
- Third-Party Risk Management Policy
- Data Classification and Handling Standard
- Information Security Policy

14. Review

The Director of Learning reviews this procedure annually or following any breach that reveals a material gap. Changes are reviewed by the Privacy Officer and the Chief Executive Officer before publication.

15. Document Control

Document Owner: Director of Learning

Review Authority: Chief Executive Officer

Review Frequency: Annual

Next Review Date: To be set on first publication

Owner review items

The drafting process identified the following in the supplied answers. Resolve each before customer release.

Type	Detail	Where
gap	The applicable privacy statute and its notification deadline are not specified in the information supplied. Ontario organisations may be subject to PIPEDA, Ontario-specific legislation, or sector regulation. The procedure requires the Privacy Officer to confirm the applicable law and deadline for each breach, but Riverstem Learning must obtain independent legal review to determine which statute applies and what notification timeline it imposes.	Section 5.3 Step 13, Section 5.4 Step 16

gap	The Records Retention and Disposal Policy is listed as an existing document, but its retention period for breach records is not provided. The procedure references that policy for retention; Riverstem Learning must confirm the period is set and is adequate for regulatory and evidentiary purposes.	Section 5.4 Step 19, Section 5.5 Step 20
gap	The procedure does not specify whether Riverstem Learning has cyber insurance or external counsel arrangements that should be activated during a breach. If such arrangements exist, the procedure should be updated to include the activation step.	Section 5.2, Section 5.4
vague	Partner school agreements are referenced as the basis for processing learner information, but the specific notification obligations to partner schools are not detailed in the information supplied. The procedure requires coordination with partner schools; Riverstem Learning should confirm that contractual obligations are reflected in Step 18.	Section 5.4 Step 18

Information the organization must supply

These values were not available from the intake and are required before this document can operate:

- Obtain independent legal review to confirm the applicable privacy statute (PIPEDA, Ontario legislation, or sector-specific regulation) and the statutory notification deadline for breaches creating a real risk of significant harm. The procedure currently requires the Privacy Officer to determine this per breach; a standing determination would reduce response time.
- Confirm the retention period for breach records in the Records Retention and Disposal Policy and ensure it meets regulatory and evidentiary requirements.
- Set the target period for completing breach assessments. The procedure references a target but does not set one; 72 hours from acknowledgement is a common position for non-Critical breaches.
- Set the target period for completing the breach record after closure. 30 calendar days is offered as a starting point.
- Set the reporting cycle for breach metrics. Quarterly is offered as a starting point.
- Confirm whether cyber insurance or external counsel arrangements exist and, if so, add the activation step to the procedure.
- Review partner school agreements to confirm notification obligations and update Step 18 if contractual requirements differ from the current text.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.