**Post-Incident Review & Continuous Improvement (Portfolio Pack)**

**Module 8G**

**Context:** Spanish secondary (ESO/Bachillerato; ages 12-18). Aligns with GDPR accountability and EU AI Act quality management expectations (Article 17) and serious-incident learning practice.

**Post-Incident Review (PIR) Template**

**School:**  
**Department/Class:**  
**AI System:** (name, provider, version)  
**Date of Incident:**  
**Reported By:** (name/role)  
**PIR Meeting Date:**  
**Participants:** (roles)

**1) Executive Summary (≤120 words)**

What happened, who/what was affected, current status.

**2) Timeline (UTC+01:00 / local)**

* **T0 - Detection:** (date/time, by whom, how)
* **T1 - Containment:** (what was disabled/isolated)
* **T2 - Stakeholder comms:** (who informed; staff/parents/students/regulators)
* **T3 - Fix/Workaround:** (what changed)
* **T4 - Closure:** (date/time)

Attach artefacts: screenshots, tickets, emails, provider notices.

**3) Impact Assessment**

* **Individuals affected (counts):**
* **Data involved:** (categories; any special category data)
* **Harm/risks:** (educational, privacy, wellbeing)
* **Operational disruption:** (lessons, assessments, services)

**4) Compliance Check**

* **GDPR personal data breach?** (Y/N; rationale)
* **DPA notification within 72h required?** (Y/N; rationale; ref # if filed)
* **AI Act “serious incident” (high-risk AI) likely?** (Y/N; rationale)
* **Provider notified?** (Y/N; date/time; ticket/reference)
* **Contractual notice duties met?** (Y/N)

**5) Root Cause Analysis (RCA)**

Use **5 Whys** and/or fault tree:

1. Why #1 →
2. Why #2 →
3. Why #3 →
4. Why #4 →
5. Why #5 →

**Primary cause(s):**  
**Contributing factor(s):** (process, training, vendor change, config, context shift)

**6) What Went Well**

(E.g. rapid detection, clear ownership, timely comms.)

**7) What Needs Improvement**

(E.g. unclear escalation path, missing test, slow vendor response.)

**8) Actions (Corrective & Preventive)**

| **#** | **Action** | **Type (C/P)** | **Owner** | **Due** | **Status** | **Evidence/Link** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 |  |  |  |  |  |  |

**9) Stakeholder Follow-Up**

* **Closure notes sent to:** (staff/parents/students) dates/links
* **Support offered:** (counsellor, office hours, FAQ)
* **Feedback channel:** (form/email)

**10) Lessons & Policy Updates**

Reference entries made in **Policy\_Update\_Changelog.md**.

**PIR Approval:** (name/role/date)  
**Next review:** (date)

**Incidents/PIR Report EduScan 11thGrade\_English 2025-10-03**

**Post-Incident Review (PIR) - EduScan Essay Feedback Bug**

**School:** IES Rivera (Upper Secondary)  
**Dept/Class:** 1º Bachillerato – English (11th grade, ages 16-17)  
**AI System:** EduScan Essay Feedback Assistant (v3.7; Acme Learning, EU cluster)  
**Incident Date:** 2025-10-03  
**Reported By:** Laura Gómez (English teacher)  
**PIR Meeting:** 2025-10-08  
**Participants:** AI Governance Officer, DPO, IT Coordinator, HoD English, Class Tutor, Provider Success Manager (guest)

**1) Executive Summary**

During an English essay assignment, students viewing AI comments saw **peer-specific private annotations** (intended only for each student). Exposure lasted ~50 minutes before access was disabled. **27 students** in 1º Bachillerato potentially viewed others’ private feedback. No special category data was present, but privacy expectations were breached. System access was paused; provider issued a hotfix; targeted parent/student comms completed. No known external dissemination beyond classroom screenshots (deleted).

**2) Timeline**

* **T0 – 10:18** Teacher observes Student A viewing comments referencing Student B; raises with IT via Teams “Urgent”.
* **T1 – 10:26** IT disables EduScan student access (kept teacher view). Containment initiated.
* **T2 – 11:05** AI Gov Officer notifies provider; ticket #AL-32491; requests incident RCA & patch.
* **T3 – 12:30** Internal heads-up to staff in English Dept; parent holding note drafted (not sent yet).
* **T4 – 15:10** Provider confirms mis-scoped caching layer after v3.7 patch; deploys hotfix EU-edge.
* **T5 – 16:00** Class debriefs with students; screenshots deleted in class with teacher oversight.
* **T6 – 18:00** Parent notice sent to the 27 affected families; DPO contact provided.
* **T7 – 2025-10-05 09:00** Limited student access restored under monitored “single-user sandbox” mode.
* **T8 – 2025-10-08** PIR held; actions agreed.

Evidence: IT ticket #INC-5751; provider note; parent email PDF; class attendance and deletion confirmation.

**3) Impact Assessment**

* **Individuals:** 27 students affected; potential peer-to-peer visibility of comments.
* **Data:** Names, essay text, AI formative comments aligned to each student; **no health/biometric data**.
* **Harm/Risks:** Privacy upset; potential embarrassment; moderate trust impact.
* **Operations:** 1 class disrupted; tool paused for 2 days across English Dept.

**4) Compliance Check**

* **GDPR personal data breach?** **Yes.** Unauthorized disclosure to other students in the class.
* **DPA notification (72h)?** **No** (documented rationale): risk assessed as **low-to-moderate** - limited audience, short exposure, immediate containment, no special category data, and verified deletion of screenshots in-class. **Action:** recorded in breach register with rationale.
* **AI Act serious incident (high-risk)?** **No.** Tool supports formative feedback; no grading/placement decisions; no fundamental-rights harm identified.
* **Provider notified?** **Yes**, 2025-10-03 11:05; ticket #AL-32491.
* **Contractual notice duties:** **Met** (24h clause).

**5) Root Cause Analysis (5 Whys)**

1. **Why** were peer comments visible? → Shared cache returned last rendered comment thread.
2. **Why** was cache shared? → Edge cache key omitted student\_id in v3.7 optimization.
3. **Why** wasn’t this caught in testing? → Staging used single-user test accounts; no concurrent student sessions.
4. **Why** didn’t we detect on rollout? → No canary class + no automated E2E test for multi-student isolation.
5. **Why** no canary/E2E? → Internal deployment checklist didn’t require class-level concurrency tests for provider hotfixes.

**Primary causes:** Provider code regression (cache keying).  
**Contributing factors:** Our lack of canary pilot & E2E multi-student isolation test; quick enablement of minor update without sandbox.

**6) What Went Well**

* Teacher spotted and escalated immediately.
* Fast containment (8 minutes to disable student access).
* Calm classroom management; deletion of screenshots supervised.
* Clear parent communication same day; DPO contact provided.
* Provider RCA + hotfix delivered same day.

**7) What Needs Improvement**

* Add **canary class** protocol for any AI update.
* Introduce **automated isolation test** before re-enable.
* Tighten change-control: “minor” provider updates still require local validation.
* Pre-approved **parent comms templates** for privacy incidents.

**8) Actions**

| **#** | **Action** | **Type** | **Owner** | **Due** | **Status** | **Evidence** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Add canary rollout (1 class) for any AI update before full enablement | P | AI Gov Officer | 2025-10-15 | Open | SOP v1.2 draft |
| 2 | Build E2E test: multi-student isolation check (unique cache keys) | C | IT Coordinator | 2025-10-22 | In progress | GitLab MR #219 |
| 3 | Update English Dept playbook: rollback & comms templates | P | HoD English | 2025-10-18 | Open | Draft in SharePoint |
| 4 | Vendor contract addendum: require pre-prod multi-user test evidence for edge/caching mods | P | Business Manager | 2025-11-01 | Open | Legal ticket LEG-44 |
| 5 | Staff refresher: how to spot/report privacy incidents (10-min micro-CPD) | P | DPO | 2025-10-25 | Planned | CPD slide deck |

**9) Stakeholder Follow-Up**

* **Parents/students:** Closure note (2025-10-10) confirming hotfix + safeguards added; DPO contact.
* **Staff:** Dept briefing and updated SOP.
* **Feedback channel:** incidents@insrivera.edu (monitored).

**10) Lessons & Policy Updates**

Recorded in **Policy\_Update\_Changelog.md**: canary rollout requirement; E2E test gate; template pack for comms.

**PIR Approved:** AI Governance Officer (2025-10-08)  
**Next Review:** Action progress check on 2025-11-05

**/incidents/CI\_Action\_Log.md**

**Continuous Improvement: Action Log (Incidents & Audits)**

| **ID** | **Source (Incident/**  **Audit)** | **Action** | **Category** | **Owner** | **Opened** | **Due** | **Status** | **Outcome/Link** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CI-001 | PIR-EduScan-2025-10-03 | Introduce canary class for AI updates | Process | AI Gov Officer | 2025-10-08 | 2025-10-15 | Open | SOP v1.2 draft |
| CI-002 | PIR-EduScan-2025-10-03 | E2E multi-student isolation test | Technical | IT Coordinator | 2025-10-08 | 2025-10-22 | In progress | GitLab MR #219 |
| CI-003 | PIR-EduScan-2025-10-03 | Comms templates (parents/staff) | Comms | HoD English | 2025-10-08 | 2025-10-18 | Open | /comms/templates |
| CI-004 | PIR-EduScan-2025-10-03 | Contract addendum: pre-prod test evidence | Procurement | Business Manager | 2025-10-08 | 2025-11-01 | Open | LEG-44 |
| CI-005 | Monitoring Q3 | Add “teacher-agreement with AI suggestions” KPI to dashboard | Metrics | AI Gov Officer | 2025-10-01 | 2025-10-20 | Planned | Dashboard v0.3 |

**Statuses:** Planned / In progress / Blocked / Done (with link)

**Incidents/Policy Update Changelog**

**Policy & Procedure Update Changelog (Incidents → Improvements)**

| **Date** | **Trigger** | **Policy/Doc** | **Change Summary** | **Owner** | **Version** | **Link** |
| --- | --- | --- | --- | --- | --- | --- |
| 2025-10-09 | PIR-EduScan-2025-10-03 | AI Change Control SOP | Added **canary class** pilot & **local E2E isolation test** as mandatory gates before re-enable; clarified rollback steps. | AI Gov Officer | v1.2 | /policies/ai\_change\_control\_v1\_2.md |
| 2025-10-12 | PIR-EduScan-2025-10-03 | Parent/Staff Comms Pack | New **privacy incident templates** (holding note, closure note, FAQ); translation checklist (ES/EN). | HoD English | v1.0 | /comms/templates/ |
| 2025-10-20 | PIR-EduScan-2025-10-03 | Vendor Contract Addendum | Require **pre-prod multi-user test evidence** for caching/edge changes; 24h incident notice reaffirmed. |  |  |  |