**Notification & Reporting Pack (GDPR + EU AI Act)**

**Module 8E**

**School context:** Spanish secondary school (ESO → Bachillerato, ages 12-18).  
**Role:** AI Governance Officer.  
**Scope:** High-risk educational AI and any systems processing personal data.

**1) Quick Decision Tree (text)**

1. **Did personal data get accessed/altered/lost by unauthorised parties?**
   * **Yes → GDPR breach flow.**
     + Risk to individuals’ rights/freedoms likely? → **Notify DPA within 72h** + **inform affected individuals without undue delay.**
     + Low/no risk? → **Document internally** (no external notice), keep breach register.
   * **No → go to 2.**
2. **Is a *high-risk AI system* involved and did the event plausibly cause serious harm or a fundamental-rights impact?**  
   Examples: unfair grading at scale; discriminatory placement; invasive biometric misuse.
   * **Yes → AI Act serious incident flow.**
     + **Inform provider immediately.**
     + **Provider (or deployer where applicable) notifies national AI Market Surveillance Authority (MSA) within 15 days** (earlier if severe).
   * **No → log and handle internally.**
3. **Child-safeguarding or criminality?** (e.g. grooming, extortion, platform intrusion)
   * **Yes → immediate law-enforcement contact** + parallel GDPR/AI-Act actions if applicable.

**Notes (Spain):** DPA is **AEPD**. The AI MSA will be the **national AI authority designated by Spain** (e.g., AESIA subject to formal designation). Keep contacts updated in your register.

**2) Timelines at a glance**

* **GDPR - Supervisory Authority (AEPD):** notify **within 72 hours** of awareness if risk likely.
* **GDPR –-Affected Individuals:** **without undue delay** if **high risk** to individuals.
* **EU AI Act – Serious Incident:** **provider (or deployer where applicable)** notifies **MSA within 15 days** of awareness (earlier for critical cases).
* **Vendor → School (processor → controller):** **“without undue delay.”** (Contractual DPA clause - Article 28 GDPR.)
* **Law enforcement / Child protection:** **immediate** for safety-critical events.

**3) Roles & RACI (suggested)**

| **Task** | **AI Gov Officer** | **DPO** | **IT/Sec** | **Principal** | **Vendor** | **Comms/Legal** |
| --- | --- | --- | --- | --- | --- | --- |
| Initial triage & classification | R | C | C | I | I | I |
| Containment (disable/patch) | C | I | R | I | C | I |
| GDPR risk assessment | C | R | C | I | C | I |
| Notify AEPD | C | R | C | I | I | C |
| Notify AI MSA (AI Act) | C | C | C | I | **R** (provider) | C |
| Notify affected individuals | C | R | I | A | I | C |
| External press statement | I | C | I | A | C | R |
| Evidence pack / logs | C | C | R | I | C | I |

*A = Approver, R = Responsible, C = Consulted, I = Informed.*

**4) Contact Register (placeholders)**

| **Authority / Partner** | **Contact** | **Channel** | **Hours / Notes** |
| --- | --- | --- | --- |
| **AEPD (Spain DPA)** | [Name/desk] | [email/portal/phone] | Breach reporting (72h) |
| **AI MSA (Spain)** | [TBD, keep updated] | [email/portal] | AI Act serious incidents |
| **Local Police / Child Protection** | [Unit/contact] | [phone/email] | Immediate for safeguarding |
| **Vendor – Primary Incident Contact** | [Name] | [email/phone] | Contract: 24/7 notification |
| **Cloud/Hosting (if separate)** | [Name] | [email/phone] | SLA |
| **School Legal Counsel** | [Name] | [email/phone] | Review templates |
| **Comms Officer** | [Name] | [email/phone] | Parent/media comms |

(Stored alongside with incident plan and **review this each term**.)

**5) Templates**

**A) GDPR Supervisory Authority Notice (AEPD) - Template**

**Subject:** Personal data breach notification - INS Premià de Mar, [Date]

* **Controller:** INS Premià de Mar, [Address], [Contact]
* **DPO contact:** [Name, email, phone]
* **Date/time breach discovered:** [dd/mm/yyyy hh:mm]
* **Nature of breach:** [unauthorised access / disclosure / loss / alteration]
* **Categories of personal data:** [names, emails, grades, comments …]
* **Data subjects affected:** [number], ages [range] (students/staff)
* **Likely consequences:** [privacy impact, distress, reputation risk]
* **Mitigation/containment taken:** [disabled system, patched bug, reset permissions, logging…]
* **Measures to address / prevent recurrence:** [vendor fix, code review, policy update, training]
* **Notification to data subjects:** [date/plan or justification if not required]
* **Cross-border aspects:** [if any]
* **Attachments:** incident log, technical notes, evidence screenshots, processor incident notice

*Signed:*  
Maria-Antònia Guardiola, Data Protection Officer, INS Premià de Mar

**B) GDPR - Parent/Student Notice (plain-language)**

**Subject:** Important: incident involving your child’s school data

Dear families,

We are writing to inform you that on **[date]**, a software issue in an English class tool briefly allowed some students to view **peer feedback comments** that should have been private. We **fixed the issue immediately** and took the system offline while we investigated.

* **What data:** teacher feedback comments linked to first name and class. No passwords, IDs, or contact details were exposed.
* **Who saw it:** other students in the same class for a short period.
* **What we’ve done:** patched the software, added extra checks, and reviewed access controls with the vendor.
* **Support:** if your child has concerns, please contact **[counsellor/contact]**.
* **Questions:** our DPO **[name]** is available at **[email/phone]**.

We regret this incident and are taking further steps to prevent a repeat. Thank you for your understanding.

Sincerely,  
[Principal Name], Principal - INS Premià de Mar

**C) EU AI Act - Serious Incident Notification (Provider/Deployer)**

**Subject:** Serious incident report - High-risk educational AI - [System Name], [Date]

* **System & version:** [Name, version], provider [Company], deployer [School]
* **Use case (Annex III education):** [grading/placement/assessment…]
* **Date/time & location:** [dd/mm/yyyy hh:mm], [City/School]
* **Description:** [What happened; how discovered; scope]
* **Suspected impact category:** ☐ Health/physical harm ☐ Critical infrastructure ☐ **Fundamental rights impact** ☐ Other serious harm
* **Persons affected:** [est. number], ages [range]
* **Immediate measures:** [paused system, human review added]
* **Investigation status:** [ongoing / preliminary cause]
* **Corrective actions planned:** [model rollback/retrain, configuration change, documentation updates]
* **Liaison with other authorities:** [e.g., DPA notified under GDPR on dd/mm]
* **Evidence/logs:** [available on request; secure repository reference]

*Submitted by:*  
[Provider contact OR Deployer if applicable], [role], [contact]

**D) Vendor Incident Notice - Contractual (Art. 28 GDPR)**

**Subject:** Urgent: Processor incident notice - [System], [School]

Per our DPA terms, please confirm **within 24 hours**:

* Summary of the incident and detection time
* Data categories and data subjects affected
* Root cause (preliminary) and containment steps
* Whether data left the EU / third-party sub-processors involved
* Timeline for permanent fix and customer communication support
* Point of contact for coordinated notifications

Regards,  
[AI Governance Officer], for INS Premià de Mar  
[contact]

**6) Worked Example (Spanish high-school, 11th-grade English)**

**Scenario:** A software bug in an AI-assisted feedback tool exposed **peer feedback comments** among students in **1º Bachillerato English** for ~30 minutes during class.

**Classification:** **Level 3 (Serious)** - confidentiality breach; minors; risk of embarrassment/peer impact.

**Actions & Notifications**

* **Containment (T0):** Teacher disables tool; IT revokes access; vendor alerted.
* **Awareness (T+1h):** Incident team convened; logs preserved.
* **GDPR risk assessment (T+6h):** Risk to rights/freedoms **likely** (minors’ personal data).
* **AEPD notice (≤72h):** DPO files breach notification; includes mitigation and parent notice plan.
* **Affected individuals (asap):** Parents/students informed (plain-language letter above).
* **Vendor coordination:** Root cause patch; QA validation before re-enable.
* **Post-incident review (T+7d):** Add pre-release test for permissions; teacher refresher; update breach register.

**Not an AI Act serious incident** (no fundamental-rights systemic harm), so **no MSA notice** required. (Document this rationale.)