**Assignment: AI Incident Response Plan**

**Module 8D**

**Applies to:** High school (ESO 1–4; Bachillerato 1–2), English department exemplar but school-wide by design.

**1) Roles & contact sheet**

| **Role** | **Primary** | **Backup** | **Responsibilities** |
| --- | --- | --- | --- |
| Incident Coordinator (AI Lead) | … | … | Activate plan, classify, chair calls, timeline & log. |
| Data Protection Officer (DPO) | … | … | GDPR triage, DPA notifications, records. |
| Safeguarding Lead | … | … | Child protection actions & external referrals. |
| IT/Security Lead | … | … | Containment, forensics, access revokes, vendor tech bridge. |
| Comms Lead (Principal/Comms Officer) | … | … | Internal & external comms, media lines. |
| Tool Owner (Dept.) | … | … | System context, user coordination, manual workarounds. |
| Legal Counsel (as needed) | … | … | Regulatory and contractual advice. |

*(A one-page appendix with phone, mobile, email and after-hours escalation shall be added for full tracking).*

**2) Activation criteria**

* Any event classified **L2-L4** (see 8C matrix).
* Any suspicion of **personal data breach** or **child safety** issue.
* Any **systemic fairness** issue affecting grades/admissions/support decisions.

**3) First 24 hours (runbook)**

**T+0–30 minutes - Stabilise & capture**

* Stop harm: disable affected feature/system; revoke tokens; isolate endpoints.
* Preserve evidence: export system logs, capture screenshots, note exact timestamps, keep originals read-only.

**T+30–60 minutes - Classify & assign**

* Apply the 8C scorecard; set **L1–L4**; assign Incident ID & owner; open incident log.
* Convene response huddle (Coordinator, DPO, IT, Tool Owner, Comms, Safeguarding as needed).

**T+1–4 hours - Contain & notify**

* Containment actions executed (rollback/update/geo-block; switch to manual process).
* **Notify per level** (see matrix). For suspected GDPR breach, DPO starts 72h timer.
* Inform vendor; request named incident manager & RCA timeline.
* Draft holding statements (internal staff; parents if L3–L4).

**T+4–24 hours - Investigate & communicate**

* Root-cause working theory; identify affected data/people; confirm scope.
* Decide on **GDPR notification** (DPA ≤ 72h) and **AI Act serious incident** escalation (provider/MSA ≤ 15 days) if applicable.
* Send parent/student comms (L3–L4); open support inbox/FAQ.
* Agree temporary controls and re-enable plan (if safe).

**4) Containment playbooks (pick & adapt)**

* **Data leak (web/app):** Take service offline or switch to maintenance; rotate keys; invalidate sessions; snapshot DB; block offending endpoints/IPs; engage vendor SOC.
* **Biased outputs/grading:** Suspend automated decision feature; enforce human-in-loop validation; freeze affected grades; announce review/appeal path.
* **Unauthorized access (stranger in class/game):** Kill session/invite; audit access lists; rotate codes; inform safeguarding & parents; preserve chat logs for police.
* **Toxic chatbot response:** Disable bot; content-filter hardening; require human escalation for sensitive topics; proactive welfare check for affected student.

**5) Notification pathways (checklist)**

**GDPR (personal data breach):**

* ☐ Risk assessment complete; decision logged.
* ☐ DPA notified **≤ 72h** (include nature, categories, counts, likely consequences, measures taken; DPO contact).
* ☐ Data subjects notified *without undue delay* if **high risk** (clear, plain-language letter; support offered).
* ☐ Processor↔Controller duties observed (vendor notified; Article 28 terms).

**EU AI Act (high-risk AI serious incident):**

* ☐ Provider notified immediately (if we’re deployer); request provider incident ID.
* ☐ Provider (or deployer, where applicable) to notify **Market Surveillance Authority** **ASAP / ≤ 15 days**; we supply logs/evidence.
* ☐ Cooperate in corrective actions (Article 65); document recall/suspension decisions.

**Safeguarding / law enforcement (child safety):**

* ☐ Safeguarding lead engaged; ☐ Police/child services contacted where indicated.
* ☐ Parents/guardians informed same day with welfare focus.

**6) Communication templates (editable)**

**A. Staff (internal) – first notice**  
*Subject: Immediate notice - temporary change to {System}*  
We’ve identified an incident affecting {system}. The feature {X} has been **temporarily disabled** while we investigate. Please {manual workaround}. Do **not** share details externally; direct parent/media queries to {Comms Lead}. We’ll update by {time}. - {Incident Coordinator}

**B. Parents/Guardians (GDPR breach)**  
*Subject: Important information about your child’s data*  
We’re writing to inform you of an incident on {date} involving {system}. Some personal information ({categories}) may have been accessible to unauthorized users for a short period. We have contained the issue, reported it to the Data Protection Authority, and are taking steps to prevent recurrence. We currently have **no evidence** of misuse, but we recommend {practical steps if any}. Questions: {contact}. We’re sorry this occurred and will keep you updated. - {Principal / DPO}

**C. Press holding line (if asked)**  
On {date}, {School} experienced an IT incident affecting {what}. We acted immediately to secure systems, support affected students, and notify the relevant authorities. Protecting our students’ privacy and safety is our highest priority. We will provide further updates when appropriate.

**7) Investigation, RCA & corrective actions**

* **RCA format:** Problem statement → Timeline → Technical cause(s) → Process gaps → Controls that failed → Controls added.
* **Action plan:** Owner, due date, success metric (e.g., bias disparity ↓ to <2%), verification step, stakeholder sign-off.
* **Change management:** Test → Approve → Deploy → Monitor (include rollback plan).

**8) Post-incident review (within 10 school days)**

* What worked / what didn’t (people, process, tech).
* Did we meet **72h** GDPR & **15-day** AI Act clocks? Evidence?
* Where to update: policy, training, contract clauses (e.g., breach notice SLA ≤ 24h, logs access, fairness testing), onboarding checklists.
* Share anonymized lessons with staff & governance committee; update dashboard metrics (incident count, MTTR, fairness KPIs).

**9) Appendices**

**A. Contact tree & after-hours rota**

* **B. Incident log template** (fields match 8C)
* **C. Decision tree (A3 one-pager)**: “Data involved?” → “Safety risk?” → “High-risk AI?” → route to GDPR / Police / AI Act / Internal.
* **D. Vendor expectations (contractual)**: breach notice ≤ 24h; no training on our data; system logs access; human-in-loop & override; decommissioning & deletion SLAs.