**AI Incident Response Plan Template for Schools**

**1. Incident Classification Matrix**

Define three severity levels with clear, school-specific examples:

| **Level** | **Classification** | **Examples** |
| --- | --- | --- |
| **Level 1 – Low** | Minor operational glitch | UI delays, non-sensitive data display errors, minor performance issues |
| **Level 2 – Medium** | Privacy-moderate or low-impact bias | Exposure of non-sensitive student data within small groups |
| **Level 3 – High** | Safety risk or fundamental rights impact | Exposure of sensitive data (e.g. special needs), biased access allocation, system failure during emergency (see etienne) |

These align with GDPR’s definition of personal data breach risk and the EU AI Act’s "serious incident" thresholds (e.g. fundamental rights violations or safety incidents)

**2. Roles & Responsibilities**

* **Incident Response Lead** (Principal or IT Director): Overall coordination.
* **IT/Technical Lead**: Manages containment, diagnosis and vendor communication.
* **Data Protection Officer (DPO)**: Regulatory compliance, breach assessment & reporting.
* **Communications Lead**: Stakeholder messaging (parents, staff, media).
* **Vendor Liaison / Compliance Lead**: Interfaces with AI provider and regulatory bodies (e.g. market surveillance authority under EU AI Act)

**3. Response Workflow**

1. **Detection**: Staff, systems, or audits flag incidents.
2. **Reporting**: Incident documented and escalated to Incident Response Lead.
3. **Containment**: Technical measures to stop further harm (e.g. suspend system).
4. **Classification**: Assign severity level using matrix.
5. **Notifications**:
   * **Internal**: Inform leadership, IT, DPO, Communications.
   * **External**:
     + For personal data breaches: DPO assesses. If risk is likely → notify Data Protection Authority within 72 hours and affected parties promptly (GDPR Art. 33).
     + For High‑risk AI serious incidents → notify vendor immediately, and regulatory authority within 15 days (or faster for severe/widespread cases) as required by EU AI Act Article 73
6. **Resolution**: Apply fixes and corrective actions.
7. **Documentation**: Log all actions, dates, decisions, and communications.
8. **Post-Incident Review**: Within 7-14 days, conduct lessons learned, update policies, assign and track corrective tasks.

**4. Notification Procedures**

* **Student Data Breach**: DPO to notify GDPR authority within 72 hours, inform families without undue delay.
* **High-risk AI Incident**: Incident Lead and DPO coordinate with vendor; determine if reporting to Market Surveillance Authority is needed under EU AI Act (serious incident rules).
* **Template use**: Keep pre-defined notice templates for incident types (e.g. data breach, safety fault).

**5. Communication Plan**

* **Spokesperson**: Principal or designated Communications Lead.
* **Audience & Methods**:
  + **Parents/Students**: Clear, empathetic emails or letters.
  + **Staff**: Briefings or internal memos.
  + **Media**: Pre-prepared statements approved by leadership when needed.
* Workflow: Communications Lead drafts → Incident Lead approves → Release.

**6. Post-Incident Review**

* **Timeline**: Hold debrief within 10 working days.
* **Participants**: Incident team members.
* **Deliverables**:
  + Root cause analysis.
  + Action plan (e.g., system updates, training, plan revisions).
  + Schedule for follow-up and ensure closure of action items.

**7. Regulatory Alignment**

* **GDPR – Article 33**: Breach notification within 72 hours to supervisory authority.
* **EU AI Act – Article 73**: Serious high‑risk AI incidents must be reported within 15 days (sooner for very serious or widespread cases)
* **Governance & Documentation**: Maintain detailed records per both GDPR and AI Act to demonstrate accountability, fairness, human oversight, and continuous monitoring

**Flowchart** describing the AI Incident Response Workflow:

┌───────────────────┐

│ 1. Incident │

│ Detection │

└─────────┬─────────┘

│

┌─────────▼─────────┐

│ 2. Reporting to │

│ Incident Lead │

└─────────┬─────────┘

│

┌─────────▼─────────┐

│ 3. Containment │

│ (Suspend or Limit │

│ the Affected AI) │

└─────────┬─────────┘

│

┌─────────▼─────────┐

│ 4. Classification │

│ (Low / Medium / │

│ High) │

└─────────┬─────────┘

│

┌─────────▼───────────────────────────────────┐

│ 5. Investigation & Preservation │

│ • Gather logs / evidence │

│ • Root cause & vendor analysis │

└─────────┬───────────────────────────────────┘

│

┌─────────▼────────────────────────┐

│ 6. Notifications │

│ - Low: Internal team only │

│ - Medium: Internal + parents │

│ - High: + DPO, GDPR authority, │

│ Market Surveillance Authority │

│ (as required by GDPR / EU AI Act) │

└─────────┬────────────────────────┘

│

┌─────────▼─────────┐

│ 7. Resolution & │

│ Mitigation │

│ (Patches, fixes, │

│ updated access, │

│ model retraining) │

└─────────┬─────────┘

│

┌─────────▼─────────┐

│ 8. Recovery & │

│ Restoration │

│ (Re-enable AI, │

│ monitor with care)│

└─────────┬─────────┘

│

┌─────────▼─────────┐

│ 9. Documentation │

│ & Logging │

│ (Incident log, │

│ communications, │

│ timeline, roles) │

└─────────┬─────────┘

│

┌─────────▼─────────┐

│10. Post-Incident │

│ Review (“Lessons │

│ Learned”) │

│ → Update plan, │

│ assign tasks, │

│ train staff │

└───────────────────┘