Module 8I: Portfolio Activity
AI Incident Response Plan

Incident Classification Criteria/Matrix

Criteria	Evidence	Severity
Scope and scale: How many have been affected by the incident?		
Sensitivity: What type of data or system is involved?		
Impact on individuals: To what extent is this incident a harm to a student or staff member?		
Impact on operations: To what extent does it disrupt teaching or school operations?		Level 1- Minor I...
Legal/ regulatory implications: To what extent does the incident trigger legal duties (GDPR, AI Act, "serious incident" reporting)?		
Reputational Impact: To what extent does this incident draw media attention or impact community trust if not handled properly?		

Levels of Severity

Level 1- *Minor Incident:* Little to no impact on people, operations, beyond school **Example:** School's scheduling assistant double booked the computer lab, which was proactively remedied **Rationale:** No lasting harm, administrative assistant anticipated and remedied proactively, otherwise, no impact on people, operations, or broader community.	**Level 2**- *Moderate Incident:* Some impact, not disruptive **Example:** AI application went down for an hour, disrupting instruction in one classroom. A student found a minor bug that showed them another student's non-sensitive data (username). **Rationale:** Small group affected, personal, though not sensitive information revealed, limited disruption, no broader communication beyond parents of students involved.	**Level 3**- *Serious incident:* Observable impact on people or operations, likely requires broader response and external notification **Example:** A data breach of student contact info, an AI tool gives out inappropriate advice affecting student mental health, bias in an AI system that unfairly grades students **Rationale:** Sharing of personal information, automated high stakes decision making by an AI tool are examples of human rights violations. Triggers activation of the incident response team, requires communication with authorities and parents of those involved.	**Level 4**- *Critical Incident (Crisis)*: Potentially life-threatening incident or one involving national media attention **Example:** A chatbot tells a child to take his own life or a predator contact leads to a child being abducted. **Rationale:** This represents a massive failure of either an AI system or the safety protocols in place and a complete disruption to people and operations. It requires an immediate response and the inclusion of law enforcement and regulatory authorities, cooperation from providers and deployers, as well as a coordinated media and crisis communication plan.

ChatGPT was used as an editing partner for the workflow and team member descriptions, offering suggestions for refinement and additional detail to my initial drafts.

Module 8I: Portfolio Activity
AI Incident Response Plan

Incident Response Team

Incident Response Role	Name	Email + Phone
Lead: Coordinates Incident Response and Decision Making		
Communications Coordinator: Approves and delivers all internally and externally-facing communications surrounding the incident. May appoint others to deliver messages who may have a relationship with the recipients, but will provide talking points.		
Technical Coordinator: Manages the technical assessment and containment of the AI system incident, coordinates with IT staff and vendors, oversees any necessary system shutdowns or configurations.		
Student Welfare Officer: Focuses on student well-being, assessing potential harm to students, and coordinates with counseling services or child protection as needed.		
Legal/Compliance Advisor: Advises on legal or compliance issues that arise as a result of the incident and what needs to be disclosed to the authorities and families and when.		
Data Privacy Officer: Manages concerns about student data protection, coordinates with communication coordinator to notify appropriate stakeholders about privacy breaches and how to mitigate.		

ChatGPT was used as an editing partner for the workflow and team member descriptions, offering suggestions for refinement and additional detail to my initial drafts.

Module 8I: Portfolio Activity
AI Incident Response Plan

Incident Response Workflow

Detection & Reporting

- **Incident Identified**
  (e.g., inappropriate AI-generated content, data exposure via AI tool, biased AI output, cheating, etc.)

- **Report Submitted to AI/Tech Lead or Incident Response Team (IRT)**
  (Staff, student, or system flags the incident using a standardized form or email protocols

2. Classification & Escalation

- Classify the Incident using the Incident Classification Matrix

- Activate Incident Response Team if Level 3 or Level 4 Incident
- Notify School/District Leaders, Legal, Parents (as needed)

3. Containment & Investigation

- **Secure Systems & Data**
  (e.g., suspend access to affected AI tool, preserve evidence)

- **Conduct Internal Investigation**

    - Gather facts
    - Interview involved parties
    - Review system logs, AI usage data

- **Engage Experts as Needed**
    - (IT, AI ethics, legal, student services)
    - Notify authorities as appropriate

4. Resolution

- **Remediate**
    - Remove/disable tool
    - Apply disciplinary policies (if applicable)
    - Provide support to affected individuals

- **Communicate Resolution**

ChatGPT was used as an editing partner for the workflow and team member descriptions, offering suggestions for refinement and additional detail to my initial drafts.

- Notify all stakeholders of the incident, what happened, and actions taken to ensure transparency with staff/students/families
- If the incident involves personal data of students, the DPO will assess and, if risk is likely, notify the Data Protection Commission within 72 hours, and notify affected individuals without undue delay.
- For any serious incident involving our AI systems vendor, we will inform the vendor immediately and coordinate any required AI Act notification

5. Review & Learn

- **Post-Incident Review (within 5–10 days)**
  - What went wrong/right?
  - Was the response effective?
  - How did our workflow hold up?
  - How can we prevent recurrence?

- **Update Policies/Trainings/Tools/Resources as appropriate**

- **Document Lessons Learned & Close the Incident**

ChatGPT was used as an editing partner for the workflow and team member descriptions, offering suggestions for refinement and additional detail to my initial drafts.