



School of Coding & AI

Student First Always

HIGHER EDUCATION

Incident Response Protocol

Policy Owner: Suki Gill

Full Name	Position	Signature	Date	Review Cycle
Suki Gill	Principal		01.09.2025	Annual

School of Coding Limited T/A School of Coding & AI
Company Number: 10808021 Registered in England & Wales
Registered Address: Unit 8-8b, Newton Court, Westrand, Pendeford Business Park,
Wolverhampton, WV9 5HB



1. Introduction

The Incident Response Protocol is designed to ensure a swift, coordinated, and efficient approach to managing and resolving incidents at School of Coding & AI HE. This protocol outlines the steps to be followed to address and mitigate any adverse events that could compromise the safety, security, or integrity of our students, staff, data, and infrastructure.

2. Scope

This protocol applies to all incidents, including but not limited to:

- IT security breaches
- Health and safety incidents
- Data breaches or loss
- Physical security breaches
- Disruption to services or operations

3. Objectives

The objectives of this protocol are to:

- Provide clear steps for reporting and managing incidents
- Minimise the impact of incidents on the Institute 's operations
- Ensure the safety and well-being of students, staff, and visitors
- Safeguard sensitive information and Institute assets
- Ensure compliance with legal and regulatory requirements

4. Roles and Responsibilities

- Incident Coordinator: Leads the incident response process and ensures that all relevant parties are informed and coordinated.
- IT Security Team: Manages incidents related to data breaches, cyber threats, or IT systems failures.
- Health and Safety Officer: Oversees the response to physical safety incidents, ensuring compliance with safety regulations.
- Data Protection Officer: Responsible for incidents involving personal data breaches and ensuring adherence to GDPR.
- Incident Response Team (IRT): A designated team responsible for executing the protocol in response to incidents, including representatives from IT, HR, and Facilities.



5. Incident Reporting

- Immediate Reporting: Any person who witnesses or becomes aware of an incident must report it immediately to their line manager or the relevant department (IT, Health and Safety, or Facilities).
- Incident Log: All reported incidents must be recorded in the Incident Log by the responsible team, detailing the nature, time, and individuals involved in the incident.

6. Incident Response Procedure

Step 1: Identification

- Identify the type of incident and assess its potential impact.
- Categorise the incident according to its severity: minor, moderate, or major.

Step 2: Containment

- Isolate the issue to prevent further damage. This could involve disconnecting compromised systems, securing affected areas, or evacuating personnel.
- Ensure that the situation is safe before proceeding.

Step 3: Notification

- Notify the Incident Coordinator, who will inform the Incident Response Team (IRT).
- Inform affected stakeholders, including students, staff, and external parties if necessary.
- For serious incidents, notify external authorities such as the police, local health authorities, or the Information Commissioner's Office (ICO) for data breaches.

Step 4: Investigation

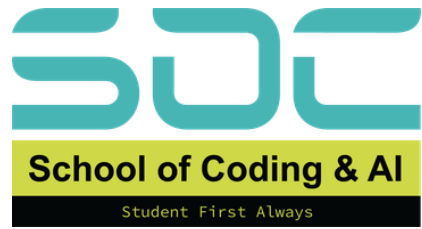
- Investigate the root cause of the incident. The IRT will gather evidence, interview witnesses, and review logs or other relevant data.
- Document all findings and ensure the integrity of any evidence for potential legal or regulatory action.

Step 5: Resolution

- Implement immediate remedial actions to resolve the incident and restore normal operations.
- Coordinate with external specialists if required, such as IT security experts, emergency services, or legal advisors.

Step 6: Post-Incident Review

- Conduct a full post-incident review to evaluate the effectiveness of the response.
- Document lessons learned and recommend improvements to prevent recurrence.
- Report findings to the senior management team and, where applicable, regulatory bodies.



7. Communication Plan

Effective communication is essential during any incident. The Incident Coordinator will ensure that:

- Internal Communication: Staff, students, and management are kept informed of incident status and any required actions.
- External Communication: Relevant authorities, suppliers, or external stakeholders are notified promptly if their services or operations are affected.

8. Training and Awareness

All staff must be aware of this protocol and their roles in incident response. School of Coding & AI HE will conduct regular training sessions to ensure readiness and familiarity with the procedures.

9. Regular Review of Protocol

This protocol will be reviewed annually, or after any major incident, to ensure it remains effective and aligned with best practices and regulatory requirements.