Corporate Ref.	CD 004
Level	3
Senior Responsible Officer	Director of Communications, Policy & Research
Version	6
EIA	18/03/2024
Approved by	Audit and Risk Assurance Committee
Approved date	22/05/2024
Superseded version	5
Review date	22/05/2025

Edinburgh College

Critical Incident Management

Policy and Procedure

Communication, Policy, and Research

Version Control

Version	Author	Date	Changes
5	Information Manager	09/04/2024	Added EIA date.
6	Portfolio Manager	31/01/2024	Updated branding, process review, contact lists

1. Purpose and scope

The purpose of this policy is to assist Edinburgh College staff to manage the response to a critical incident.

A critical incident is defined as: "Any incident which is likely to have a serious impact on a student/s, staff member/s, people working in the College, key stakeholders, or the reputation of the College."

The College's CIM policy and procedure aligns to the new international standard IS22301, which states:

"In any critical incident situation there should be a simple and quickly formed structure that will enable the organisation to:

- Confirm the nature and extent of the critical incident.
- Take control of the situation.
- Contain the incident.
- Communicate with stakeholders."

2. Incident notification and escalation

If an incident happens at the College where **there is a serious threat to life, safety or wellbeing, or a serious criminal act is in process or has occurred**, staff must notify the police in the first instance.

- Emergency – call 999
- Non-emergency medical – call 111
- Non-emergency police – call 101

Critical incidents are to be escalated to a direct line manager and Senior Management Team (SMT) member to determine if further escalation to the Executive Team is required.

If the **critical incident involves a loss of personal data or a cyber threat/attack**, it should be escalated to the Information Management or Digital Infrastructure Service Lead. They will then assess whether further escalation to the Chief Operating Officer is necessary, and the College's Cyber Incident Response Plan (CIRP) will be activated. This CIM policy and procedure does not supersede College emergency response procedures i.e. fire evacuation.

If contact with an Executive team member is not possible, staff may call the College's business continuity lead - Portfolio Manager, Emma Miller on 01312 978 113.

Once notification has been received by the Executive team member, they will make an assessment on the severity of the incident, and then decide whether to call a Critical Incident and establish a Critical Incident Management team (CIM Team), who may then invoke a range of actions and/or business continuity management plans.

3. Critical incident management procedure

The purpose of the critical incident management procedure is to enable the College to react as effectively and efficiently as possible to a critical incident, in a coordinated and well managed manner, and to communicate well with all affected or interested parties.

Once the Executive team member receives notification of an incident, they must make an initial risk assessment of the severity of the incident.

The table below is a guide to quickly assess the severity of the incident, which utilises a simple 1-3 risk-based scoring system.

This may act as a formal record of the assessment, so due care and attention should be taken when assessing.

Executive team members are encouraged to discuss the assessment with other senior colleagues, if possible, to inform their assessment:

ASSESSMENT THEME	SCORE 1= low risk 2 = medium risk 3 = high risk
1. Is there a serious threat to life or safety for students, staff, or visitors?	
2. Is there a serious risk to student, staff, or visitor wellbeing?	
3. Is there a serious risk to the College's ability to deliver learning, teaching and assessment?	
4. Is there a serious risk to the College's ability to operate its estate?	
5. Is there a serious risk to the College's ability to deliver student services?	
6. Is there a serious risk to the College's ability to operate its IT systems?	
7. Is there a serious risk to the College's reputation?	
Total	**/ 21**

If the total risk is below 13, then the incident does not need to be named as critical and operational actions/plans will suffice.

If the total risk is 13 or above, then the Executive team member should formally name the incident a critical incident, and the critical incident procedure, indicated below, must be invoked:

CRITICAL INCIDENT PROCEDURE			
STEP 1: Response set-up & personnel			
1.1 Strategic lead (GOLD) assigned	**1.2 Establish critical incident management (CIM) team**	**1.3 Appoint tactical lead (SILVER)**	**1.4 Response location established**
The Executive team member to either take on the role for the critical incident (CI) or appoint another senior manager *Note: The GOLD lead will act as a single point of contact for external agencies, like the police media or other significant stakeholders, who require contact with the college about the incident*	The GOLD lead identifies and informs members of the CIM team who will assess in more detail the impact on the College and agree a range of actions to manage the incident *Note: Business continuity management plans will list the GOLD, SILVER and BRONZE members for certain CI*	The GOLD lead may also appoint a SILVER lead in the event of a complex critical incident to assist in assessing impacts and managing the CIM team response. The other members of the CIM team will be BRONZE command. *Note: Command definitions outlined in Appendix 6*	Team to agree if a central location from which the CIM team can operate is needed. This will depend on the significance or impact of the incident *Note: The Estates management team can advise on these matters*
STEP 2: Action			
2.1 CIM team to meet	**2.2 Decided if business continuity management (BCM) plan needed**	**2.3 Funding**	**2.4 Deliver actions**
To discuss options and agree/record actions to respond to the CI *Note: A decision log should be maintained throughout the life of*	The CIM team to agree if a BCM plan is appropriate to invoke *Note: BCM plans available on college intranet and in red folders*	Approval for emergency funds should be sought if needed to respond to the critical event *Note: The CIM team must ensure that all associated costs are recorded on the decision log*	As agreed by the CIM team *Note: The primary purpose of the CIM team is to return the*

the incident – See Appendix 1 for decision log template			*college to a business-as-usual state, as soon as possible*
STEP 3: Closure			
3.1 RECOVERY ASSESSMENT The CIM team to assess if a 'business-as-usual' state has been sustained and any remaining risks or impacts have been successfully managed, the GOLD lead may close the CI			
STEP 4: Lessons learnt			
4.1 A CRITICAL INCIDENT REPORT TO BE COMPLETED The GOLD lead and the Director of Communications, Policy & Research to write up a report for review and approval by the Executive and Senior Management Teams *Note: Critical incident report template is available*			
STEP 5: Review			
5.1 DOCUMENTS REVIEWED Once the critical incident report has been approved all relevant documentation should be sent to the Portfolio Manager in the Communication, Policy & Research department for appropriate storage The Portfolio manager will assess the lessons learnt and any other recommendations to make appropriate amendments to any associated plans, policies, or procedures.			

4. Policy governance and review

The Portfolio Manager serves as the accountable officer for this policy. An annual review process is undertaken and involves assessments conducted through both the Executive team and Senior Management team (SMT) before the commencement of each academic year. The responsibility for policy implementation rests with both the Executive team and SMT.

5. Appendix 1 – CIM team decision log template

DATE	TIME	ASSESSED IMPACT OR RISK	ACTION OPTIONS	AGREED ACTION AND OWNER	PROGRESS UPDATE

(NB. one option maybe to invoke a business continuity management plan, indicated at Appendix 2 below)

6. Appendix 2 – Business continuity plans

NB. Plans are published on the college intranet and printed in red folders in the boardroom and at reception on each campus.

PLAN NAME	PLAN OWNER	DEPUTY
Loss of Site or Loss of Access to Site	Chief Operating Officer	Director of Finance & Infrastructure
Loss of Utilities	Chief Operating Officer	Director of Finance & Infrastructure
Terrorist Threat/Attack	Executive team	Director of Finance & Infrastructure
Pandemic	VP of Corporate Development	H&S Manager
Adverse Weather	Executive team	Director of Finance & Infrastructure
National Power Outage	Executive team member on site at each campus	SMT member on site at each campus
Critical System – iTrent	Director of HR & OD	HR Systems Analyst
Critical System – Agresso	Director of Finance	Finance Manager
Critical System – Unit e	Assistant Principal Quality & Improvement	MIS Manager

Critical System – My EC	Development Service Lead – Business Solutions Development Team	IT Business Solutions Developer
Critical System - Celcat	Assistant Principal Quality & Improvement	College Timetabling & Accommodation Officer