Corporate Ref.	CD 004
Level	3
Senior Responsible Officer	Portfolio Manager
Version	5
EIA	18/03/2024
Approved by	Audit & Risk Assurance Committee
Approved date	22/02/2023
Superseded version	4
Review date	22/02/2024

Edinburgh College

Critical Incident Management

Policy and procedure

Version Control

Version	Author	Date	Changes
5	Information Manager	09/04/2024	Added EIA date.

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

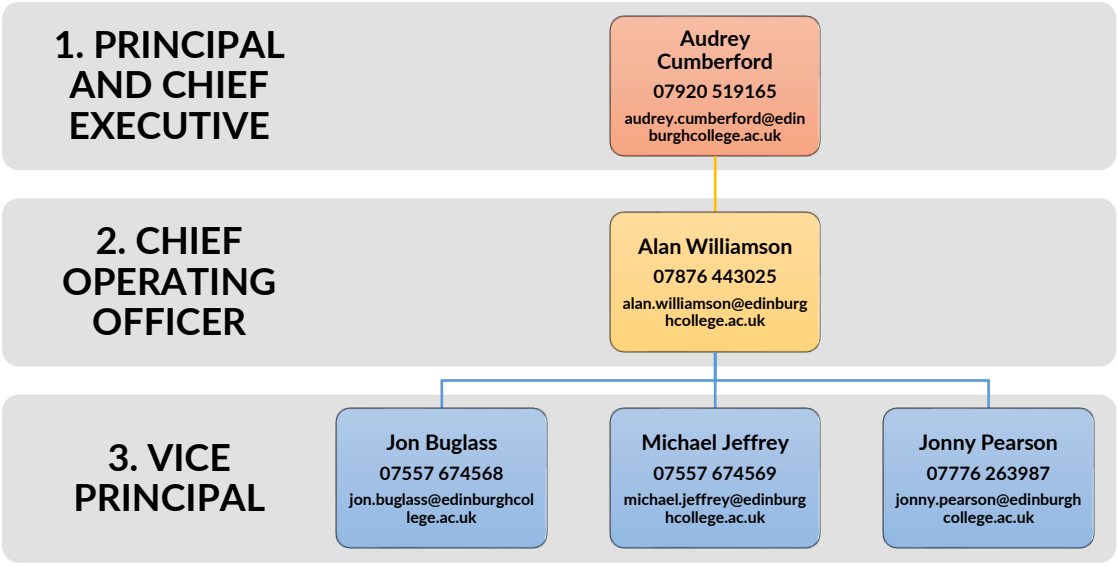
If an incident happens at the College where there is a serious threat to life, safety or wellbeing, or a serious criminal act is in process or has occurred, staff must notify the police in the first instance.

- 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 is related to a loss of personal data or cyber threat/attack**, then escalation should be directed to the Information Management or IT team who will then determine if further escalation should be made to the Chief Operating Officer.

This CIM policy and procedure does not supersede College emergency response procedures i.e. fire evacuation.
Executive team escalation tree:



If contact with any of the above Executive team members is not possible, staff may call the College's business continuity lead - Director of Communications, Policy and Research, Nick Croft on 07969 955386.

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	The GOLD lead to assign members of the CIM team who will assess in more detail the impact on the college and agree a range of actins to manage the incident	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	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 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	*Note: Business continuity management plans will list the CIM team members for certain CI*	*Note: Typically, only needed for CI's which have high risks to normal college operations*	*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 incident – See Appendix 1 for decision log template*	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 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 accountable officer for this policy is the Director of Communications, Policy and Research, who will review this policy through the Executive team and Senior Management team (SMT) on an annual basis, prior to the beginning of each academic year.

Responsibility for implementing the policy sits with 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

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

PLAN NO	PLAN NAME	PLAN OWNER	DEPUTY	LAST REVIEW	NEXT REVIEW
1	Cyber Attack	Chief Operating Officer	Gordon Hope Graham Inglis	April 2021	2023
2	Loss of Site or Loss of Access to Site	Chief Operating Officer	Dave Keen Colin McLaren	November 2022	November 2023
3	Loss of Utilities	Chief Operating Officer	Dave Keen Colin McLaren	November 2022	November 2023
4	Terrorist Threat/Attack	Executive Team	Dave Keen Colin McLaren	October 2022	October 2023

5	Pandemic	VP of Corporate Development	Andy Bamberry	October 2022	October 2023
6	Adverse Weather	Executive Team	Dave Keen Colin McLaren	October 2022	October 2023

7. APPENDIX 3 – COMMUNICATION CONTACTS

COMPANY/AREA	CONTACT NAME(S)	TELEPHONE NUMBER(S)	WEB ADDRESS/EMAIL
Scottish Fire and Rescue Service	Emergency Sighthill Granton Milton Midlothian	999 0131 442 1420 0131 332 6315 0131 669 5110 0131 660 2619	www.firescotland.gov.uk
Police Scotland	Emergency Non-emergency	999 101	www.scotland.police.uk
Scottish Ambulance Service	Emergency National HQ Divisional HQ	999 0131 314 0000 0131 314 0137	www.scottishambulance.co.uk
Radio stations	Radio Forth	0131 556 9255	www.forth1.com
	Heart Radio	0141 781 1011	www.heart.co.uk
	Borders Radio	0189 675 1010	www.radioborders.com
Scottish Funding Council	Outcome Agreement Manager Seamus Spencer	0131 313 6673	www.sfc.ac.uk
Scottish Qualifications Authority	Regional Manager Theresa McGowan	0774 103 7255	www.sqa.org.uk theresa.mcgowan@sqa.org.uk
Zurich Municipal	Kirsty Forsyth	0141 204 7010 07767 225537	www.zurich.co.uk kirsty.forsyth@uk.zurich.com
Estates Management team	Estates Manager - TBC (all estate)		
	Dave Keen (Granton and Milton Road)	07734 948032	dave.keen@edinburghcollege.ac.uk
	Colin McLaren (Sighthill and Midlothian	07989 132080	colin.mclaren@edinburghcollege.ac.uk

COMPANY/AREA	CONTACT NAME(S)	TELEPHONE NUMBER(S)	WEB ADDRESS/EMAIL
Public Health	Public Health Protection Team (Duty System)	0131 465 5420 Out of hours service: 0131 242 1000	Na
Colleges Scotland	Head of Communication & Public Affairs – Will McLeish	0178 689 2100 0771 240 4397	will.mcleish@collegesscotland.au.uk

8. APPENDIX 4 – KEY DOCUMENTS AND FILES

DOCUMENT OR FILE NAME	LOCATION (S)	FORMAT	DOCUMENT OWNER
CIM Policy and Procedure (this document)	Reception - Premises Information Folders	Hard Copy	Portfolio Manager
	Boardroom – Red folders	Hard Copy	Portfolio Manager
	Offsite with key members of staff	Hard Copy	Portfolio Manager Director of Communications, Policy, and Research
	Office 365 Teams – dedicated Critical Incident and Business continuity Teams site	Soft copy – Word	Portfolio Manager
	Staff Intranet - EC Staff Intranet (edinburghcollege.ac.uk)	Soft copy - PDF	Portfolio Manager
Site Plans	Local network drives (S) - S:\Estates Services\Private\Resources and Facilities\Floor Plans Estates - One Drive	AutoCAD (soft) or PDF	Facilities Managers
	Reception - Premises Information Folders	Hard Copy	Facilities Managers
	Boardroom – Red folders	Hard Copy	Facilities Managers
	Offsite with key members of staff	Hard Copy	Facilities Managers Director of Communications, Policy, and Research
Business Continuity Management Plans (BCM Plans)	All campus boardrooms	Hard Copy	Portfolio Manager
	Office 365 Teams – dedicated Critical Incident and Business continuity Teams site	Soft copies – Word	Portfolio Manager

	Staff Intranet - EC Staff Intranet (edinburghcollege.ac.uk)	Soft copies - PDF	Portfolio Manager
	Offsite with key members of staff	Hard Copy	Portfolio Manager Director of Communications, Policy, and Research