Corporate Ref.	CD 004
Level	3
Senior Responsible Officer	Nick Croft
Version	3
Approved by	SMT
Approval date	27 Jan 2022
Superseded Version	2
Review date	February 2023

Edinburgh College

For the future you want

Critical Incident Management

Policy and Procedure

Corporate Development

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 Critical Incident Management (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:

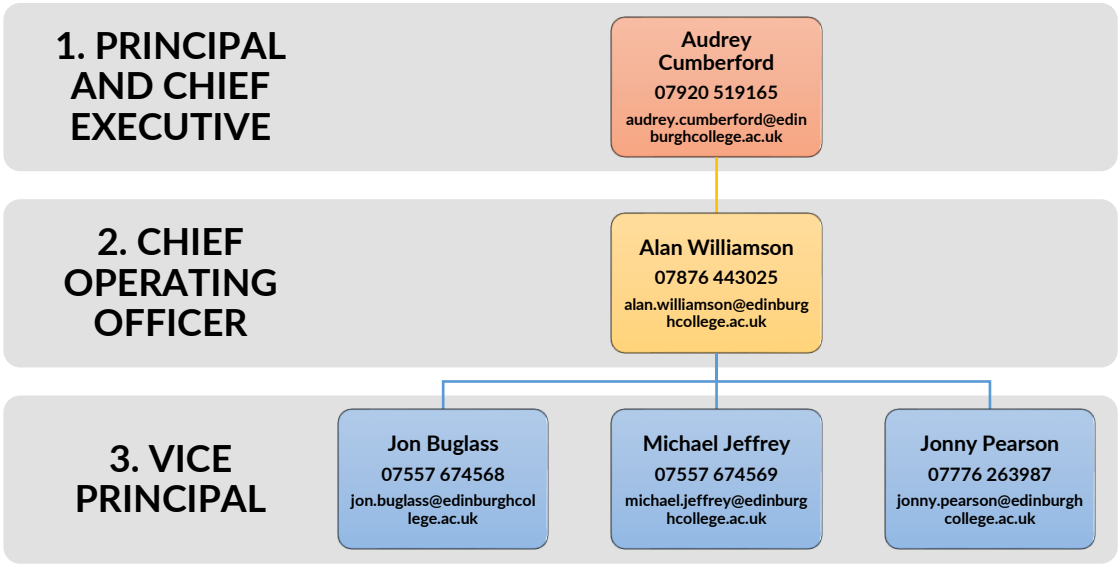
- Confirm the nature and extent of the critical incident.
- Take control of the situation.
- Contain the incident.
- Communicate with stakeholders.”

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, using 999.

If the critical incident is related to a loss of personal data or cyber threat/attack, then escalation should be directed to the Chief Operating Officer by the incident lead in the Information Management or IT team.

Thereafter, staff must contact the Executive team members indicated in the order identified below:



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**
- Thereafter the staff member must notify their line manager

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, who may then invoke a range of actions, business continuity management plans, and/or critical incident 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 (table below) 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 Setup & Personnel

1.1 STRATEGIC LEAD (GOLD) ASSIGNED:
The Executive team member has to either take on this role for the critical incident, appoint another Executive or Senior Manager.

The Strategic Lead (Gold) 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 critical incident.

1.2 ESTABLISH CRITICAL INCIDENT MANAGEMENT (CIM) TEAM:
The Strategic Lead (Gold) to assign members of and chair team. Team will assess in more detail the impact on the College, and discuss, then agree, a range of actions to manage the critical incident.

This may involve invoking one of the **business continuity management** plans the College has in place.

1.3 APPOINT TACTICAL LEAD (SLIVER):
The Strategic Lead (Gold) may also appoint a Tactical Lead (Silver) in the event of a complex critical incident to assist in assessing impacts, and managing the Critical Incident Management team response.

Typically only needed for CI's with identified high risks to College business

1.4 RESPONSE LOCATION ESTABLISHED:
Team to agree if a response location from which the CIM team can operate is needed. This will depend on the significance or impact of the critical incident.

The Estates team managers can advise on these matters and their contact details are listed in Appendix 4.

STEP 2: Action

2.1 CIM TEAM TO MEET:
The CIM team should meet as soon as possible to discuss options, and agree and record actions, to respond to the incident

A Decision LOG should be maintained throughout the life of the incident – **See Appendix 1 for a copy of the CIM Decisions Log template**

2.2 DECIDE IF BUSINESS CONTINUITY MANAGEMENT (BCM) PLAN NEEDED:
The CIM team may choose, as part of its agreed actions, to invoke an existing BCM Plan

BCM Plans available on College intranet and in red folders: List plans
Once invoked, steps will be outlined in BCM Plan

2.3 FUNDING:
Approval for emergency funds can be sought from the Chief Operating Officer, Head of Finance or Principal and Chief Executive

The CIM team must ensure that all associated costs are recorded on the Decision LOG, as it may not have access to purchase order systems

2.4 ADDITIONAL SUPPORT:
Business and administrative support will be provided by the Executive Support team (Trish Hanlon) or Governance team (Marcus Walker) to assist with a response venue, calling and ensuring participation of members of the CIM team, and recording issues, options and actions on the Decision LOG.

2.5 TAKE ACTION:
As agreed by the CIM Team

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:
Once the CIM team assesses that a 'business as usual state' has been sustained, and any remaining risks or impacts have been successfully managed, the Strategic Lead (Gold) may close the CIM team.

STEP 4: Lessons Learnt

4.1 A MAJOR INCIDENT REPORT TO BE COMPLETED:
The Strategic Lead (Gold) and the Director of Communications, Policy and Research, for review and approval by the Executive team and Senior Management team (SMT).

STEP 5: Review

5.1 DOCUMENTS REVIEWED:
Once the Major Incident Report has been approved all relevant documentation, must be sent to the Director of Communications, Policy and Research, for storage and review

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 and on an annual basis, prior to the beginning of each academic year.

Responsibility for implementing the policy sits with Executive team and Senior Management Team.

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 3 below)

6. APPENDIX 2 – BUSINESS CONTINUITY PLANS

NB. Plans are published on the college intranet and printed in 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	April 2022
2	Loss of Site or Loss of Access to Site	Chief Operating Officer	Dave Keen Colin McLaren	October 2021	October 2022
3	Loss of Utilities	Chief Operating Officer	Dave Keen Colin McLaren	October 2021	October 2022
4	Terrorist Threat/Attack	Executive Team	Dave Keen Colin McLaren	August 2021	August 2022
5	Pandemic	Vice Principal of Corporate Development	Andy Bamberry	August 2021	August 2022
6	Adverse Weather	Executive team	Dave Keen Colin McLaren	April 2021	April 2022

7. 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