Incident Response Guidance (DRAFT – v1.0 – January 2022)

1.0 Incident Definitions

1.1 Critical Incident – Operational Response - Bronze Command – RAG Status Green

A Critical Incident will require a routine response by specialist local team(s) as part of their normal operations. The University's primary responders in such incidents will normally be Security or Residential Life, in collaboration with Student Wellbeing Services and SEF Support Services. Escalation will not be necessary to manage the response and recovery and no additional resources will be required. Such incidents will be overseen by a Site Incident Manager, depending on the type of incident this will be the Head of Security, the Head of Residential Life or the SEF General Manager. The Site Incident Manager will act as Bronze Commander, notify relevant other departments/stakeholders and escalate to senior commanders, as necessary. The relevant teams will have documented plans in place in order to respond to such incidents and alert other internal departments.

Examples of Critical Incidents may include:

- an isolated incident involving harm or distress to an individual (on or off campus)
- denial of access or damage to small part of a building (single-room failure)
- short-term evacuation due to temporary safety cordon or alarm (shelter not required)

1.2 Significant Incident – Tactical Response - Silver Command - RAG Status Amber

A Significant Incident is likely to require a coordinated response from within numerous Professional Services/Schools to supplement the aforementioned operational arrangements. There may be disruption affecting several schools and services across the University. Specific 'local' plans may need to be invoked to manage the incident and additional resources may be required to support the tactical response. Silver Commanders will be appointed by the affected PS Divisions and Schools (in accordance with local Emergency/BC Plans) so as to co-ordinate response and recovery activities and to provide information for internal and external communications about the incident.

Examples of Significant Incidents may include:

- hazardous conditions on Campus (e.g. chemical spill, severe weather, disruptive protest)
- IT or utility outage – restoration/recovery of service expected within 8 hours

1.3 Major Incident – Strategic Response - Gold Command - RAG Status Red

A Major Incident will have a University-wide impact requiring a strategic response by the University's senior leaders. Major incidents are likely to cause prolonged disruption to the University's activities. The COO will act as the University's Gold Commander and the University Incident Management Team (UIMT) will oversee decision-making during the incident response and secure resources to support recovery. The University's Crisis Communications Plan will be invoked to manage internal and external information about the incident and to monitor and respond to media coverage. Further details can be found in the University BC Plan.

Examples of Major Incidents may include:

- incident involving multiple casualties within the University's care (locally or overseas)
- explosion, fire or flood damages building(s), infrastructure and/or the environment
- large-scale, evacuation due to life-threatening hazard (emergency shelter required)
- cyber-attack causes prolonged disruption to IT systems and/or reportable data breach
- outbreak of life-threatening pandemic illness within the University community (e.g. Meningitis)

2.0 Command, Control and Communication

2.1 Incident Escalation Process – Bronze, Silver and Gold Command

During the initial response phase, the Site Incident Manager (Bronze Commander) will review the impact of the incident and if necessary, the overall management of the incident will be escalated to Silver and/or Gold Command. The diagram below shows the escalation process, for use when the Site Incident Manager (Bronze Commander) requires tactical advice and/or strategic decision-making in order to effectively manage an incident.
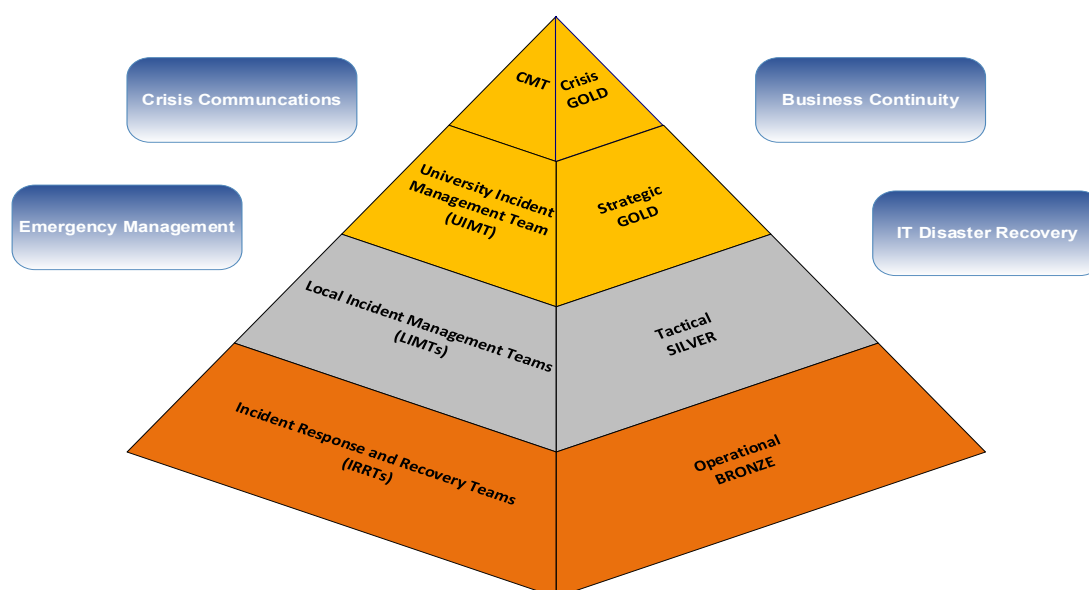

Student Incident
Security (3333)

SEF Head of Security
Head of Wellbeing/
Residential Life

Campus Incident
SEF (7777)

SEF Operations Manager
SEF Head of Campus FM
Head of Service Delivery

IT Incident
ITS (8090)

Head of IT Operations
Service Desk Manager
Cyber Security Manager

Director for the Student Experience

Director of Estates

Director of IT

- Resources
- Decisions
- Actions

Chief Operating Officer

- Resources
- Decisions
- Actions

The contact details of the above University Incident Commanders are held in the Incident Contacts Directory. NB - Incident Managers may also use WhatsApp to communicate and MS Teams to meet.

2.2 Incident Escalation – University Command Structure (Dependent on Scale of Incident – see Section 1)

Crisis Communcations

Business Continuity

Emergency Management

IT Disaster Recovery

CMT Crisis GOLD

University Incident Management Team (UIMT)

Strategic GOLD

Local Incident Management Teams (LIMTs)

Tactical SILVER

Incident Response and Recovery Teams (IRRTs)

Operational BRONZE

2.3 Situation Reporting (SITREP)

When communicating about an incident, University responders should use the Red, Amber, Green (RAG) reporting system to indicate the impact as described in the table below:

RAG Status	Incident	Description of Impact	Response required
Green	Critical	Isolated incident with no ongoing threat Short-term service disruption (< 1 day) Barely noticed by students, staff or stakeholders	Normal/ Operational (Bronze)
Amber	Significant	Schools/services activities suspended Medium-term service disruption (> 1 day) BC Plans may be invoked to support recovery	Tactical Management (Silver)
Red	Major	Loss of facilities, equipment or personnel Longer-term, University-wide disruption (2 days+) Activities suspended, prolonged recovery time	Strategic Management (Gold)

By adopting the SITREP (2.3) and METHANE (2.4) system, incident responders will be in a position to communicate consistently and coherently with the emergency reponders.
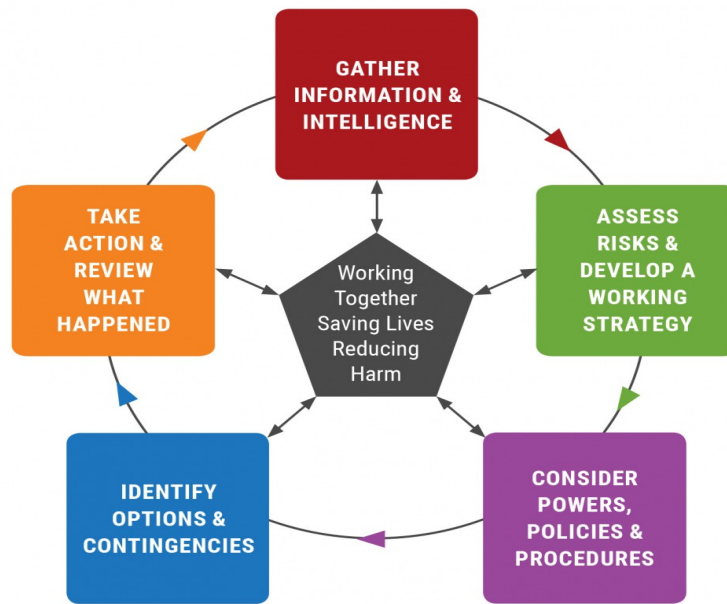
2.4 Incident Reporting (METHANE)

M	MAJOR INCIDENT	Has a major incident or standby been declared? (Yes / No - if no, then complete ETHANE message)	Include the date and time of any declaration.
E	EXACT LOCATION	What is the exact location or geographical area of the incident?	Be as precise as possible, using a system that will be understood by all responders.
T	TYPE OF INCIDENT	What kind of incident is it?	For example, flooding, fire, utility failure or disease outbreak.
H	HAZARDS	What hazards or potential hazards can be identified?	Consider the likelihood of a hazard and the potential severity of any impact.
A	ACCESS	What are the best routes for access and egress?	Include information on inaccessible routes and rendezvous points (RVPs). Remember that services need to be able to leave the scene as well as access it.
N	NUMBER OF CASUALTIES	How many casualties are there, and what condition are they in?	Use an agreed classification system such as 'P1', 'P2', 'P3' and 'dead'.
E	EMERGENCY SERVICES	Which, and how many, emergency responder assets and personnel are required or are already on-scene?	Consider whether the assets of wider emergency responders, such as local authorities or the voluntary sector, may be required.

3.0 Incident Response – Action Card

Detect and describe incident

- Initial notification - alert emergency responders, start the incident log, take Grab Bag
- Arrival at the scene, maintain safe distance and gather initial information about the incident
- Senior responsible person becomes Site Incident Manager (Bronze Commander)
- Update emergency responders using METHANE report - Is this a Major Incident?
- Notify senior (Silver/Gold) commanders and escalate if additional support is required
- Provide SITREP - describe what is happening, where and who/what has been affected

Protect life and property

- Prioritise safety at the scene and control access
- Dynamic risk assessment - monitor hazards and maintain safe distance
- Assess casualties and provide support/first aid as required
- Speak to witnesses - is anyone else believed to be injured, trapped or missing?
- Evacuate people from affected areas as necessary and provide for their immediate welfare
- Formalise safety cordon and incident control point with emergency responders, as necessary
- Liaise with emergency services to safeguard critical assets and update senior commanders

Support those afftected

- Communicate with those directly affected at the scene (e.g. displaced people)
- Be prepared to evacuate a wider area, if advised to do so by emergency services
- Arrange temporary shelter for displaced people - a place of warmth with catering, toilets etc.
- Support people who have lost access to personal belongings or critical research materials
- Alert the Communications Team to warn and inform community and respond to enquiries

Mitigate impact of incident

- Invoke Emergency/BC Plans and call out designated staff (e.g. specialist advisers)
- Continue to maintain incident log of all noteworthy events and actions taken with timelines
- Provide updated SITREPs to Silver/Gold on a regular basis
- Brief Silver/Gold Command to confirm decisions and actions
- Inform Communications Team to manage messaging - agree timing and content
- Ongoing evaluation of impact and resource requirements
- Start to develop recovery strategy

Plan for recovery

- Commence initial assessment of losses, salvage activities and ongoing risks
- Continue to inform staff, students and stakeholders about the impact and action taken
- Arrange de-brief to capture lessons learned
- Evaluate risk of future incidents
- Review incident response arrangements - resources
- Review business continuity and recovery plans - documentation

3.1 Incident Response - Decision Making Aide Memoire

3.2 Incident Response Guidance – General Principles

3.2.1 Gather and Share Information

- What has happened and how are we responding? Is this a Major Incident?
- Site Incident Manager to report the scale of the incident (SITREP). Open Incident Log.
- Is Escalation necessary? Who should be informed as a priority at this stage?
- Alert the Communications Team to inform the community and monitor media coverage.

3.2.2 Risk Assessment

- Preserve life - safety and welfare check to identify any immediate hazards or threats.
- Assess the initial impact of the incident and how the effects can be mitigated.

3.2.3 Consider Policies and Procedures - Establish Command and Control

- Establish if incident is within scope of existing policies and procedures, be prepared to adapt.
- Determine the need for escalation and technical expertise – e.g. Silver/Gold command.
- Notify key personnel as necessary, including out-of-hours notification.
- Liaise with emergency responders and agree location of Incident Control Point, as necessary.
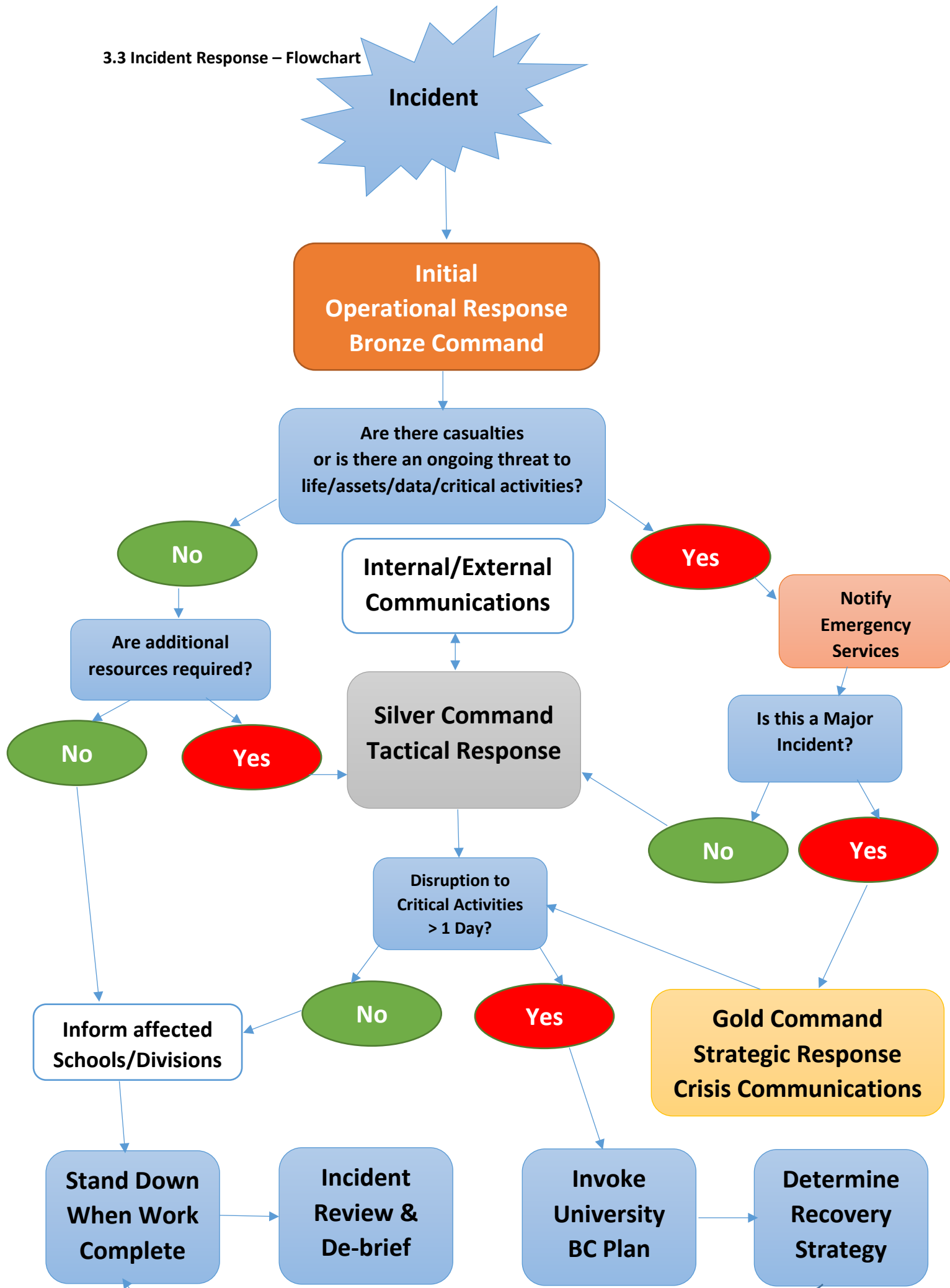
3.2.4 Objective Setting

- Prioritise the safety of personnel and identify any urgent issues for immediate action.
- Evaluate response capabilities and secure additional resources to support recovery.
- Liaise with insurers and engage with stakeholders.

3.2.5 Establish Communications Strategy

- Quickly acknowledge what has happened and inform the University community.
- Provide details of the ongoing response and recovery efforts.
- Manage the initial surge of enquiries and the flow of information.
- Monitor media coverage and provide regular updates to all stakeholders.

3.3 Incident Response – Flowchart

Incident

Initial
Operational Response
Bronze Command

Are there casualties
or is there an ongoing threat to
life/assets/data/critical activities?

No

Yes

Internal/External
Communications

Notify
Emergency
Services

Are additional
resources required?

Silver Command
Tactical Response

Is this a Major
Incident?

No

Yes

No

Yes

Disruption to
Critical Activities
> 1 Day?

Inform affected
Schools/Divisions

No

Yes

Gold Command
Strategic Response
Crisis Communications

Stand Down
When Work
Complete

Incident
Review &
De-brief

Invoke
University
BC Plan

Determine
Recovery
Strategy

4.0 Post Incident Review and Debrief

After the immediate repsonse to the incident, a post-incident review should take place to provide assurance that the Univesity has returned to 'business as usual' and to establish lessons learned.

Incident Response plans should include a 'review' section to ensure an assessement is undertaken after the event to establish why it happened, capture lessons learned to prevent a reoccurance and to enhance future arrangements.

Incident Response plans should be reviewed following any significant incident to incorporate any changes or improvements generated during the de-brief process. Where there is wider learning from an incident, these will be communicated to all Schools and Professional Services through the H&S Committee and the Risk and Resilience Management Group to ensure relevant plans have been updated.

5.0 Documentation for Reference – University Incident Response Plans

The following University-level documents contain procedures for responding to incidents:

5.1 University Business Continuity Plan – owned by GCGC

- Generic procedures and guidance for responding to emergencies and other disruptive incidents (on or off campus).
- Alignment with IT Continuity/Recovery Plans and Estates BC Plan.
- Provides framework and guidance for developing local BC Plans in Schools and PSDs

5.3 Specific Incident Response Plans

- Campus Security Response and Evacuation Plans – owned by EFM/SEF
- Severe Weather Response Plan – owned by EFM/SEF.
- Power Outage BC Plan – owned by EFM/SEF.
- Cyber/IT Incident Response and Recovery Plans – owned by ITS.
- Infectious Diseases Response Plan – owned by DSE.
- Study Abroad Placements Incident Response Plan – owned by CMA
- BC Plan for Industrial Action – owned by GCGC.
- BC Plans for critical activities such as Graduation, Open Days and Clearing – owned by CMA.
- Specific School/PSD Emergency Response and BC Plans – owned by relevant School/PSD.

5.4 Crisis Communications Plan – owned by CMA

- Procedures for managing internal and external communications during an incident.

UNIVERSITY
OF SUSSEX