Captain Cook Institute Pty Ltd trading as
George Brown College
Level 4, 56-58, York Street, Sydney NSW 2000
+612 9279 4949

Critical Incident Management Plan

Preparation for, response to, and recovery from a critical incident affecting the students and staff requires the cooperative efforts of all managers in partnership with the functional areas supporting the operations of the College.

The objectives of this Critical Incident Management Plan ("CIMP") are to make sufficient preparations for responding to a critical incident or emergency in order to minimise the effect upon the students, staff and operations of the business.

Management has a specific responsibility to respond to the needs of students in the case of a critical incident. Management also has a legal responsibility to protect its corporate resources and IT infrastructure and the information it holds. Any interruption to the normal operations of the College could be damaging to the future relationships with students and other stakeholders (including regulators) and could affect the public image of the College.

This CIMP is not designed to provide an answer to each and every type of critical incident that could happen, but rather is provided to identify the methods on how to manage a critical incident if one were to occur.

Critical incidents are extraordinary events that because of their scope, intensity or duration, overwhelm the organisation's capacity to cope and maintain equilibrium. Critical incidents may be classified as natural; such as floods, bushfires, earthquakes, and storms; or human-caused, through deliberate attack on the people or resources of the College.

This CIMP also relates to the overall emergency plans of the College and aims to minimise the damage incurred during an emergency, by providing guidelines for a rapid and effective response to an emergency situation.

The CIMP is designed to complement procedures laid down elsewhere concerning the provision of a safe environment for students and staff, regular maintenance of buildings and facilities and evacuation procedures in case of emergency. Nothing in this plan is to be taken as contrary to guidelines and procedures laid down elsewhere concerning these matters. The plan assumes that:

- Students are properly orientated in how to respond to a critical incident and what support is available to them;
- All facilities are subject to regular maintenance;
- Emergency exits are clearly marked and kept clear of obstacles at all times; fire prevention measures and protection equipment are in place (e.g. fire wardens appointed, smoke detectors, alarm systems and fire extinguishers are in place and maintained);
- Normal safe work practices are followed routinely, and staff are familiar with fire drill and emergency evacuation procedures; and
- Back-ups of computer records are stored off-site and retrievable.

Examples of critical incidents

- The death or critical injury of a staff member, student or visitor on College premises or outings.
- The destruction of whole or part of premises that the College occupies (e.g. by fire).
- The threat of damage to premises that the College occupies (e.g. a bomb threat).
- Staff and/or students being taken hostage.
- A break-in accompanied by major vandalism.
- A natural or other major disaster in the community.

CIMP & Overseas Students

The National Code defines a 'critical incident' as "a traumatic event, or the threat of such (within or outside Australia), which causes extreme stress, fear or injury". George Brown College has in place a structured approach in responding to critical incidents as they occur, and provides appropriate support and counselling services to overseas students.

Examples of Critical Incidents that may specifically affect overseas could include, but are not limited to:

- Death of a student or close family member residing in Australia.
- Attempted suicide of a student.
- Life threatening illness/injury of a student.
- Sexual and/or physical assault of a student.
- Missing student.
- Severe verbal or psychological aggression.
- Issues such as domestic violence, drug or alcohol abuse.

George Brown College will ensure that all students are made aware at their orientation of; What to do in the case of a critical incident. The point of contact for any issues which require student support, including critical incidents. The College will also ensure that where required, and as appropriate: As soon as practical after a critical incident occurs, Department of Education and Department of Home Affairs (DHA) is notified of the details of the incident including the time, location and nature of the incident. In the case of a student's death or other absence affecting the student's attendance or course progress, the incident is reported via PRISMS. That the incident and its management are recorded in each student's file.

The Plan of Action

The emphasis of this CIMP is based on three major steps:

1. Reaction
2. Recovery & Restoration
3. Review

Reaction Communication

In the case of a critical incident, it is important that key people are notified. In an emergency situation, the primary objective is the safety of human lives. Salvage and recovery operations will be of secondary importance, and will take place only when the affected area is declared safe.

When a critical incident occurs, notify the General Manager.

The General Manager may delegate to another officer to contact relevant emergency personnel as required.

Immediate response to an incident

1. Notify the responsible persons as outlined above.
2. Immediately after notification of the incident the following questions need to be addressed and recorded by the officer in charge:

- What happened?
- What makes the event critical?
- When did the incident occur?
- Where did it happen?
- Who was involved?
- Who needs assistance?
- What is the most appropriate intervention?

3. In the case that it is decided that evacuation is an appropriate intervention the evacuation plans given below should be utilised.

Recovery & Restoration

The first 24 hours

- Gather accurate facts and information.
- If possible, re-establish a sense of routine within the College. Staff members and students will feel safe once the regular patterns of management and organisation have been re-established.

The first 48 – 72 hours

- Restore routines while taking into account the needs of staff and students.
- Engage support services to manage the reactions of staff and students.
- Monitor the support services provided.
- Provide additional assistance if required and when necessary.
- Provide a formal staff meeting with professional input (if appropriate).

The first two weeks post the critical incident

- Monitor progress of those hospitalised or injured.
- Stay alert for delayed reactions from staff and students.
- Provide relevant information to those who require it.

Key actions:

- Notify all key personnel of the problem and assign them tasks focused toward recovery from the critical incident.
- Notifying students about the problem minimises panic or concern.
- Recall backups - if backup tapes are stored offsite, these need to be recalled. If using remote backup services, a network connection to the remote backup location (or the Internet) will be required.
- Organise alternate facilities in order to continue operations suppliers.
- During a critical incident, employees may be required to work longer, more stressful hours, and a support system should be in place to alleviate some of the stress. Prepare them ahead of time to ensure that work runs smoothly.
- Provide counselling opportunities and support - opportunities should be given for staff and students to discuss the incident in a supportive environment. If the incident involves death, staff and students should be apprised of funeral details and given leave to attend. Staff members are not expected to be counsellors; therefore the establishment of a counselling support appropriate to the particular critical incident is important.

Review

After the critical incident has been dealt with, it is essential that the organisation undertakes an evaluation. Evaluation of the CIMP and the roles and functions of the Coordinators and relevant support staff are an essential part of the process. Senior management should conduct a formal evaluation of the process involved in the management of the critical incident after debriefing has occurred. Formal evaluation provides opportunities for feedback on the strengths and weaknesses of the CIMP and provides an opportunity for continuous improvement. Feedback should be sought from those who have been involved in various aspects of the operation of the CIMP.

Any action taken in regard to the critical incident should be recorded along with the final evaluation of the handling of the critical incident. Where the incident, or an individual related to the incident is referred to another person or agency this should also be recorded; however, the privacy needs of individuals should also be respected in this case.

IT Infrastructure and data

Preventions against data loss

In relation to IT Infrastructure the following preventions should be implemented:

- Backups are sent off-site at regular intervals;
- Backups include software as well as all data information, to facilitate recovery;
- Use a Remote backup facility if possible, to minimise data loss;
- Utilise surge protectors - to minimise the effect of power surges on delicate electronic equipment;
- Protect servers and essential equipment with an Uninterruptible Power Supply (UPS) and/or Backup Generator;

- Fire Preventions – install effective alarm systems and accessible fire extinguishers
- Employ anti-virus software, firewalls and other security measures

Campus Evacuation
In the event of fire or bomb evacuation of the building, staff and students assemble in the courtyard at the entrance to Town Hall Station's arcade, outside the City of Sydney Library.

Students are shown the evacuation area at Orientation, during a tour that includes the library. There are only two fire stairs in the campus.

Variations

GBC reserves the right to vary, replace or terminate this policy from time to time.

Document name	Critical Incident Management Plan
Document owner	General Manager
Document approver	General Manager
Version / Issue date	V1.0 / 25 August 2017

This policy / procedure is to be reviewed a minimum of twelve (12) months from this date.

Disclaimer:
A printed copy of this document may not be the most recent version. Please check X:\GBC Central for current version