

POLICY DOCUMENT

CRITICAL INCIDENT POLICY AND PROCEDURE

1 Purpose and Scope

The purpose of this policy and its related documents is to identify the personnel, structures and procedures for managing a critical incident.

It is good practice to have documented the actions to be taken in the event of a critical incident in the form of approved policies and procedures. This includes the initial response, follow-up, reporting, review and improvement. This is also a legislative requirement of providers of education to international students.

Scope:

- All full time and part time, contract and casual staff
- All students (domestic and international)
- All visitors

2 Policy Statement

2.1 Critical Incident

A **Critical Incident** is any sudden or progressive development (event) which requires immediate attention and decisive action to prevent / minimise any negative impact on the health or welfare of one or more individuals, damage to the College's premises or disruption to the College's operations. Critical incidents may include (but are not limited to) events such as:

- Death/suicide
- Attempted suicide or self-harm
- Serious accident or life threatening injury/illness
- An absent or 'missing' international student whereby the student has not attended class and is not contactable for a certain period of time

- Severe verbal or psychological aggression
- Deprivation of liberty, threats of violence, assault, rape/sexual assault, aggravated burglary, or presence or use of biological or chemical weapons
- Domestic violence, physical, sexual or other abuse
- Child protection matters
- Fire, bomb threat, explosion, exposure to gas/chemical hazards, or discharge of firearms
- Natural disaster
- Threat of widespread infection or contamination
- Civil unrest
- Serious damage to essential facilities
- Notifiable data breach
- Cyber security threat
- Information which has the potential to negatively affect the reputation of the College in the media and/or wider community
- Any critical incident affecting students off campus while representing the College.

In general terms, a critical incident is defined as a traumatic event which causes or is likely to cause extreme physical and/or emotional distress to staff and/or students and may be regarded as outside the normal range of experience of the people affected. Every critical incident is unique and will need to be dealt with differently according to the nature and scale of the incident and the needs of the individuals affected. This policy does not apply to minor incidents for which the College provides support and assistance through Student Services and International Student Support Services.

Where College staff witness an event that may be considered a critical incident, or where staff are aware of an event which may either indicate or escalate to a critical incident, the *Critical Incident Procedures* below must be followed.

The following table provides a guide to determining the severity of critical incidents:

Level of risk:	Determined by:	Examples:
SEVERE (Emergency services required)	CEO and Dean / Associate Dean or Or Most senior member of staff available at the time	<ul style="list-style-type: none"> • Death, suicide or threat of suicide, or life- threatening injury • Deprivation of liberty, threats of violence, assault, rape/sexual assault, aggravated burglary, use of firearms, biological or chemical weapons • Fire, bomb threat, explosion, gas/chemical hazards, discharge of firearms • Threat ofwidespread infection or contamination • Natural disaster
SIGNIFICANT (Emergency Services required)	CEO and Dean / Associate Dean Or Most senior member of staff available at the time	<ul style="list-style-type: none"> • Severe workplace health and safety risk • Serious injury incurred by staff/student • 'Missing' international student • Child protection matter • Violent behaviour • Burns/alcohol/overdose/poisoning • Activity where evacuation is required • Notifiable data breaches and threats to Cyber Security
MODERATE (Emergency Services MAY be required)	CEO and Dean /Associate Dean or Or Most senior member of staff available at the time	<ul style="list-style-type: none"> • WHS risk • Suspicious package left unattended • IT System crashes • Student suffers epileptic fit or psychological breakdown

2.2 Principles

The college recognises that each incident will be unique and is committed to ensuring that each incident is managed effectively, compassionately and with the safety and welfare of all concerned being a priority.

The college aims to ensure that appropriate resources are available to respond to critical incidents, including, physical and psychological safety of affected students and staff, emotional and physical support and interventions required at different phases after an incident.

The college will keep appropriate records of critical incidents occurring and ensure that appropriate follow up actions are taken. Critical incidents will be reported to the Board by the CEO and Dean.

The level of response to a critical incident will vary depending on the circumstances and scale of the incident.

2.3 Roles and Responsibilities

- i. This policy places responsibility on **all staff** across the college. All staff must be aware of this policy and procedures for managing critical incidents. Staff may need to assume temporary control of a critical incident on site (such as calling Emergency Services, alerting other staff, assisting with first aid, crowd control etc.) until such time as relieved by the Critical Incident Officer, the Critical Incident Team or Emergency Services.
- ii. **The Critical incident officer** has responsibility for immediately controlling the situation and liaising with security or emergency services, and for obtaining the names of persons involved in the incident and documenting the details of the incident to the Critical Incident Management Team.
- iii. The Critical Incident Officer must alert the CEO and Dean or the most senior College staff member available as soon as possible who, in turn, will re-assess the situation and convene the Senior Management team if required to do so under part 2.3.1 below.
- iv. The Senior Management Team (SMT) are responsible for managing the College's **response** to any critical incident which is considered to have a severe or significant level of risk or, in some cases, moderate level of risk. The SMT is convened as soon as possible by the most senior member of staff available at the time to enable the Critical Incident Team to be formed and to plan an immediate response, allocate responsibilities and determine ongoing strategies. There may however, be instances when an effective and timely response is required and cannot be delayed to convene a critical incident team or SMT. In such instances the most senior member of staff should take appropriate action to mitigate immediate risk and advise the CEO and Dean or the most senior member of staff as soon as possible.
- v. Once the SMT is convened, the most senior staff member available becomes the **Head of the Critical Incident Team**, or assigns a suitable alternative to head the team. Taking into account the nature of the critical incident, the time available, the skills required, and availability of SMT members, the Head of the Critical Incident Team determines the Critical Incident Team membership from among the following :

- CEO and Dean
- Associate Dean
- Registrar
- Director of Student Services and Campus Wellbeing
- Heads of Department (HoDs)
- Director of Marketing and Student Recruitment
- Student Engagement and Partnerships Manager
- Compliance Officer
- Others (including the College's contractors or consultants) as deemed appropriate by the Head of the Critical Incident Team (eg. If the incident is a notifiable data breach or a cyber security issue and the college does not have a senior IT executive on site).

Where Emergency Services assume management of the critical incident, the Critical Incident Team will liaise with the managing body (e.g. Police or Fire and Emergency Services) for a coordinated approach to any response activities.

Where the College has assumed management of the critical incident, the Critical Incident Team will consult with and/or take instruction from the CEO and Dean or Board of Directors as necessary.

2.3.1 Responsibilities of the Critical Incident Team

The Critical Incidents Team's duties include, but are not limited to:

- completion of a *Critical Incident Form* outlining details such as the type of incident, the exact location and details of any person or persons who might be injured, in distress, or at risk.
- reviewing the situation, setting priorities, allocating tasks/responsibilities and coordinating an immediate response including communications (to staff, students, families of those involved, helpers, and the media)
- organizing ongoing response/follow up (including staff and student briefing, counselling, review and reporting)
- de-briefing to evaluate response procedures and make recommendations for handling future critical incidents
- placing and maintaining records in the Critical Incident Register (maintained by the CEO and Dean or Compliance Officer).

- The CEO and Dean informing the Board of the incident.

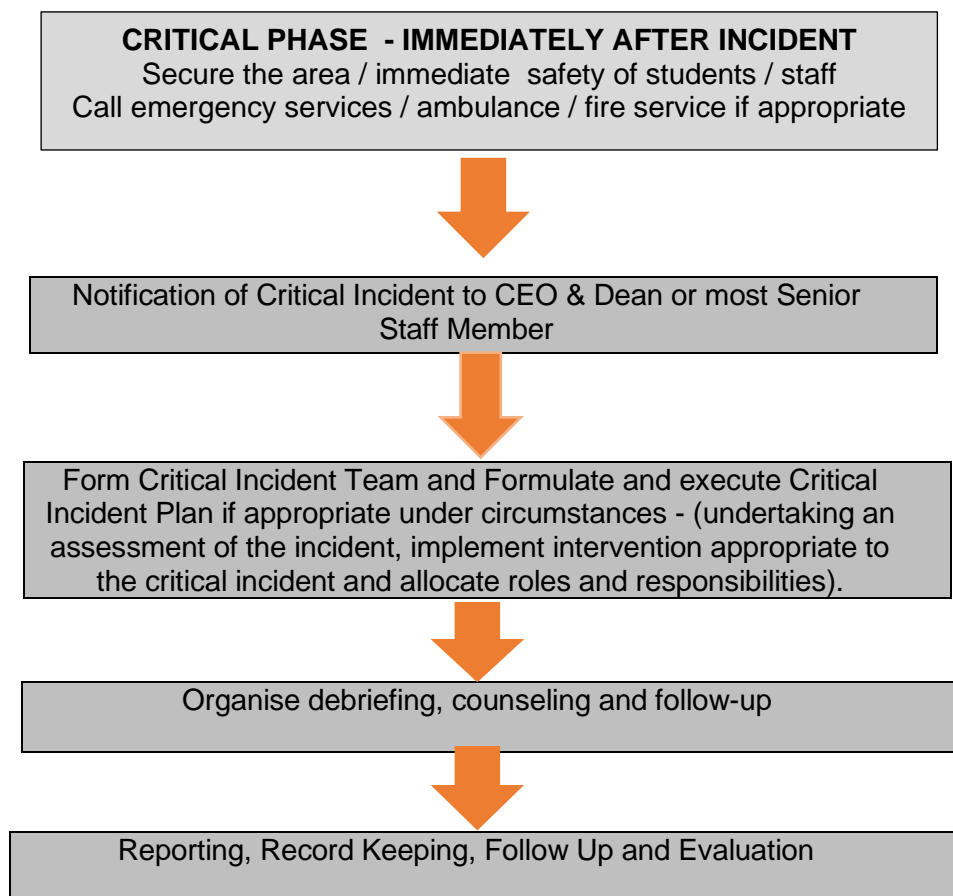
2.4 Procedure

2.4.1 Prevention and preparation

Emergency evacuation maps and notices which indicate assembly points in the event of a fire or some other threat are displayed on every floor throughout the premises. Emergency wardens are to be appointed and trained regularly in emergency and evacuation procedures. Regular evacuation exercises are to be scheduled. By means of the WHS committee safety measures are developed communicated and monitored. Staff are encouraged to report any potential safety issues or risks to management. New staff are made aware of the Critical Incident Policy and Evacuation procedures during induction.

2.4.2 Management of Critical incidents

This is summarised in the following diagram:



i. Critical Phase

The most critical phase is immediately after the incident has occurred or as soon as the College becomes aware of the imminent threat of an incident. When this occurs, the staff member who first becomes aware of the matter should:

- Ensure that the individual(s) directly affected or involved is safe and receiving appropriate medical supervision (if required) in a safe environment as a matter of priority
- Ensure that all other individuals are safe
- Report the incident to the CEO and Dean or the most senior member of staff
- The most senior member of staff will determine if evacuation procedures should be activated. In some instances there will be a need to take immediate action which will not allow the assembling of the Critical Incident Team.
- Contact the relevant emergency services and/or authorities if appropriate.
- Once the immediate danger has passed, or the individual is no longer in danger and receiving appropriate medical attention, resume activities if appropriate.
- At the earliest time, interview the individuals involved to ascertain what occurred and if there are any residual risks.
- Support other students and/or staff and arrange counselling if appropriate
- Address any other immediate needs, i.e. additional support, police statements, etc.
- Any media enquiries are to be directed to the CEO and Dean who will also liaise with the Board of Directors.

ii. Debriefing / Investigation Phase

To ensure that the incident is recorded accurately and managed the nominated Critical Incident Officer should:

- Collect facts about the incident (eg. Witness statements, injuries to any person, information from the scene). This may be captured in written form or by taking photographs.
- Examine any work or operating procedures or training that may have impacted the incident.
- Determine the cause of the accident or incident paying attention to contributing factors, environmental factors, mechanical failure, systems failure, security issues, etc.
- Review work procedures and training

- Document recommendations and provide a report to the WHS committee and the Risk and Audit Committee.

iii. Reporting Phase

Written and or verbal reports are provided to the appropriate manager including any recommendations to prevent recurrences. Any media enquiries are to be directed to the CEO and Dean. See 2.5 below.

2.5 Confidentiality and Record Keeping

All documentation relating to critical incidents will be kept confidential and shall be disclosed only to those persons who have a right to the information by virtue of their role: in the process, in relation to a student's and/or staff member's health, safety and well-being, or as required by law.

The Privacy Act 1988 (Cth) permits the College to disclose personal information about someone to a party outside the College where:

- a) A person consents in writing to their personal information being disclosed; or
- b) The College believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person/people; or
- c) The disclosure is required or permitted by law.

Written records should contain such information as is necessary for others to gain a clear understanding of the grounds upon which an incident was determined and the actions taken to address it.

Records are maintained to protect the rights and interests of all parties, explain and justify the actions of the College and its employees, and document and explain the decision-making of the College.

Details of a critical incident (including a completed *Critical Incident Form* and other evidence) are kept on the ACPE Critical Incident Register, which is maintained by the CEO and Dean and/or a Compliance Officer.

All serious incidents are reported to the Risk and Audit Committee and ultimately to the Board of Directors. Any potential further or ongoing risks are to be captured in the relevant Risk Register.

2.6 Missing International Students

Note: This section only applies to student visa holders

Where an international student is studying on a **student visa**, the College has a duty of care to ensure the student is made aware of potential risks while in Australia (e.g. beach safety and kidnapping scams) as far as possible and remains compliant with the conditions of their visa (where appropriate). As such, an international student may be classified as 'missing' if:

- The student is newly enrolled in an award course and due to start in their first study period on campus but has not arrived for their first week of classes.
- The student is a continuing student and has not re-enrolled in any subjects for the next study period and has not responded to any contact regarding enrolment by the end of the first week of that study period.
- The continuing student has enrolled in subjects but has not attended any classes on campus for two weeks without notice (at any point in the study period)
- It is brought to the attention of any staff member (academic or operational) that the student may be 'missing' either by another student, agent, family member or any other member of the community.

If an international student is classified as 'missing', the staff member who first becomes aware of the situation is to immediately contact the Registry's Office and Compliance Officer.

Steps will be taken to contact the student directly and could include (but are not limited to):

- Phone calls
- Emails
- Formal written letters
- Home visits to the last known address
- Requesting the agent responsible for the student's recruitment to contact that student.

If the student's welfare is of concern, the College reserves the right to contact the student's agent, listed next-of-kin and/or emergency contact in order to ensure that the student is safe. An international student who has not responded to any contact during the enrolment period for a period of 7 days will be sent an *Intention to Report to the Department of Home Affairs*

Notification (with option to appeal) by the College. If the international student fails to respond to any notification sent by the College regarding their absence and is classified as 'missing', the student will be reported to the *Department of Home Affairs* through the PRISMS database and the student's next-of-kin or the Police may be notified.

2.7 Critical Incident Contacts

Emergency Contacts	Contact
Police, Fire, Ambulance	000
State Emergency Service	132 500
NSW Poisons Information Centre	13 11 26
Phone-based interpreting service via Department of Homes Affairs Translating and Interpreting Service (TIS National)	13 14 50
Health Direct – 24 hour health advice line	1800 022 222
National Sexual Assault, Domestic Family Violence Counselling Service	1800 RESPECT (1800 737 732) www.1800respect.org.au
Local Hospitals	Contact
Concord Repatriation General Hospital	9767 50000 Hospital Road, Concord NSW 2139
Auburn Hospital	8759 3000 Hargrave Road, Auburn NSW 2144
St. Vincent Hospital	8382 1111 390 Victoria Street, Darlinghurst NSW 2010
Royal Prince Alfred Hospital	9515 6111 50 Missenden Road Camperdown NSW
Mental Health Support Services	Contact
NSW Mental Health Line	1800 011 511
Mensline Australia	1300 789 978
Beyond Blue	1300 224 636
Women's Information Line	1800 817 227
QLife (LGBTIQ + SUPPORT) Australia	1800 184 527
Road Trauma Support Team	1300 367 797
Lifeline	131 114
Other Useful Contacts	Contact
Department of Home Affairs	131 881 www.homeaffairs.gov.au
Overseas Ombudsman	1300 362 072 www.ombudsman.gov.au
WorkCover NSW	13 10 50 www.workcover.nsw.gov.au

3 Definitions

Convened means brought together in person, by phone, by video service or by any combination of these.

Crisis - an adverse incident or series of events that have the potential to severely damage the ACPE's people, operations, environment and its long-term prospects and/or reputation.

Critical Incident Officer – Nominated officers on campus with responsibility to control a critical incident and liaise with Security and relevant Emergency Services.

Critical Incident Management Team – Members of the Senior Management Team who assume responsibility for managing and directing the incident.

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. Application security focuses on keeping software and devices free of threats.

Cyber Security Threat – occurs when an intruder gains unauthorised access to computers, servers, mobile devices, electronic systems, networks and data from malicious attacks.

Emergency - event or circumstance that impacts on a campus' people, operations, and environment which is of a size and complexity that requires a structured response to resolve the situation'. Emergencies require the application of resources beyond that of the initial immediate response and pose higher levels of risk to ACPE.

Emergency Services – means government or other official provider of an emergency service including Police, Ambulance, Fire and Rescue and State Emergency Services .

Health is the state in which an individual does not suffer from any disease or injuries as a result of work, work activities or the work environment.

International Student: The College defines an international student or a prospective international student as a student who is not an Australian citizen, Australian permanent resident, New Zealand

citizen, or holder of an Australian permanent resident humanitarian visa, and who requires an international **student** visa from the Australian Government to study in Australia, whether applying from within Australia or from overseas.

Notifiable Data Breach – a data breach when personal information is accessed, disclosed without authorisation or lost. A data breach can harm an individual whose information is affected.

Safety is the state in which the risk of harm (to persons), damage to property or the environment is limited to an acceptable level.

Student/Learner is an individual person who is formally enrolled to study at the College. The individual person is that who appears on the College's documents such as enrolment, admission and payment documents, and who is assigned an individual student ID.

A **student visa** is a **temporary visa** which allows an international student to remain in Australia to **study** for the duration of their course. Courses types range from general english courses to university level courses. There are seven streams within the one **Student Visa**: Higher Education; Postgraduate Research, VET (Vocational Education and Training) , Schools, Independent ELICOS, Foreign Affairs or Defence, and Non-award (Ref: *Overseas students in Australian higher education: a quick guide*, 20 June 2019 -

https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1819/Quick_Guides/OverseasStudents. Under Australian Migration Regulations, in order to be granted a **student** visa for study in Australia, the applicant for the visa must:

- be enrolled full-time in an [approved Commonwealth Register of Institutions and Courses for Overseas Students](#) (CRICOS) course (that is, a course approved to be offered to overseas students)
- have sufficient money to support living in Australia
- have adequate health insurance (OSHC)
- be a 'genuine temporary entrant' with the intention to return home after studying, and meet English language requirements

Study Period – A “study period” is defined in the National Code as “a discrete period of study” in a course, namely, semester, trimester, short course or as otherwise defined by the College as long as that period does not exceed 24 weeks”. This will normally reflect the period during which the student can normally be expected to complete a group of units. A study period may also refer to the delivery period of an online subject.

4 Related Documents

- Risk and Audit Governance Framework
- Risk Registers (Principal, Operational and Academic)
- ACPE Governance Charter
- ACPE Delegations of Authority and Authority Limits Policy
- Critical Incident Register
- WHS Policy
- WHS – Student Accident-Incident Notification Form
- Sexual Assault and Sexual Harassment Prevention Strategy
- EEO, Bullying and Harassment Policy
- Student Code of Conduct
- Staff Code of Conduct

Legislation:

- Education Services for Overseas Students Act (2000) (Cwth) (and the National Code of Practice for Providers of Education and Training to Overseas Students 2018 made under that Act)
- Tertiary Education Quality and Standards Agency Act (2011) (Cwth) (and the Higher Education Standards Framework (Threshold Standards) 2015 made under that Act)
- Work Health and Safety Act (2011) (NSW) (and the Workplace Health and Safety Regulations 2011 (NSW) made under that Act) Employees Liability Act (1991) (NSW)
- Environmentally Hazardous Chemicals Act (1985) (NSW)
- Privacy Act (1988) (Cwth) (including Schedule 1 - Australian Privacy Principles)
- Children and Young Persons (Care and Protection) Act (1998) (NSW) Child Protection (Working with Children) Act (2012) (NSW) Racial Discrimination Act (1975) (Cwth)
- Sex Discrimination Act (1984) (Cwth)
- Human Rights and Equal Opportunity Commission Act (1986) (Cwth)
- SafeWork NSW

5 Policy Administration

Policy Name & Code:			Critical Incident Policy and Procedure (POL-14)
Policy Owner:			CEO and Dean
Approval Authority:			Board of Directors. ACPE
Next Review:			September 2023
Approval Date	Effective Date	Version	Summary of changes
10 Aug 17	19 Jul 18	2	Harmonised – fully harmonised for two brands.
11 Dec 18	12 Dec 18	3	Revision date: 31 October 2018 <ul style="list-style-type: none"> • Policy de-harmonised from other SGA brands. • Policy content revised to ensure accuracy and compliance with the HESF and National Code, particularly, Standard 6.. • Policy format updated in line with the new template used for ACPE policies and procedures. • Job titles and departments updated to reflect current practices.
14 Mar 19	14 Mar 19	3.1	<ul style="list-style-type: none"> • References to Dean and Operations Director replaced with CEO and Dean. • References to Student Services and Learning Support Manager replaced with Director of Student Services and Campus Wellbeing.
15 Aug 19	16 Aug 19	3.2	Policy updated to include new section 2.6 <i>Critical Incident Contacts</i> .
24 Sep 20	29 Sep 20	4	Updated legislation Updated actions to be taken relative to the incident and timeframes. Added cyber security and notifiable breaches. Added new related documents as per the new governance charter and the Risk and Audit Framework Added Associate Dean to the Senior Management Team (SMT)

* Unless otherwise indicated, this policy will still apply beyond the review date.