Elite Education Institute Pty Ltd trading as Elite Education Institute
ABN 65 162 298 580 CRICOS Provider Code: 03390A
Head Office & Sydney CBD Campus: Level 6, 8 Quay Street, Haymarket NSW 2000
Tel: +61 2 9211 4958
Website: www.ee.edu.au Email: info@ee.edu.au

10. Critical Incident Management Policy

Purpose	Sets out the Institute's approach to managing critical incidents.
Location	The policy is maintained on owncloud (original: Pydio)- http://cloud.ee.edu.au/owncloud
Responsible executive	CEO
Responsible office	CEO's Office
Effective date	30 November 2016
Review date	30 November 2018, 30 November 2023
Modification history	Jun 2013 (v1), Nov 2016 (v2), 25 Aug 2021(v3)
Related documents	Institute Security and Safety Policy (No.13)
Authority	Approved by Council

1. Purpose

The purpose of this policy is to address the risk and consequences that may arise from critical incident and to provide a guide for an effective response to a critical incident and mitigate any future risk recurring from a similar incident.

2. Scope

This policy refers to Elite Education Institute (EEI), its staff, students and facilities. The TEQSA Threshold Standards, the National Code of Practice and Providers of Education and Training to Overseas Students (National Code 2018) requires EEI to demonstrate its compliance with the National Code 2018 at the point of CRICOS registration and throughout its CRICOS registration period.

Standard 6 of the National Code 2018 requires the Institute to support students to adjust to study and life in Australia, to achieve their learning goals and to achieve satisfactory academic progress towards meeting the learning outcomes of the course.

In order to comply with **Standard 6,** the Institute must have a documented critical incident policy together with procedures that covers the action to be taken in the event of a critical incident, required follow-up to the incident, and records of the incident and action taken.

3. Definitions

For the purposes of this procedure a critical incident is defined as:

A situation or traumatic event which causes or presents a significant risk to students and staff of EEI outside the normal range of experience of the people affected. Critical incidents encompass situations such as bodily harm, property damage, legal involvement, media activity, pandemics, natural disasters or catastrophic events, war or acts of terrorism or other unusual activity that falls outside the scope of activity undertaken by EEI.

4. Procedures

4.1. Objective

4.1.1. The Student Service and Administration Manager reporting to the Registrar is duly authorised by the Institute to manage critical incidents directly involving:

- All students on-campus;
- All staff at the Institute; and,
- Approving all distribution of information to students and staff to ensure accuracy and mitigate the risk of misinformation or rumor.

4.1.2. The Student Service and Administration Manager is the nominated Critical Incident Coordinator (CIC) and forms and manages a Critical Incident Management Team (CIMT).

4.1.3. The Student Service and Administration Manager monitors the availability of appropriate resources for managing critical incidents and the development of safety measures.

4.1.4. Training and clearly accessible and understood procedures are provided to key personnel who may be affected by critical incidents.

4.2. Procedure

4.2.1. **Phase 1: Prevention**

4.2.1.1. The prevention of critical incidents through risk identification is a major component of critical incident management. EEI will undertake Critical Incident Risk Assessment and identify key risks for EEI; document and record responses to formal complaints, allegations of misconduct, breaches of academic or research integrity and critical incidents, and:

a) Record risks, mitigation strategies and resultant risk;
b) Advise on individual plans to minimise the risks identified through such measures as education and training, improvements to Work Health and Safety (WH&S), student counselling and discipline, individualised plans for students with challenging behaviour, security measures etc.;
c) Undertake an annual audit of the resources for managing key risks and report any shortfall to the Principal;
d) Approve the Risks and Prevention Checklist;
e) Ensure all International students at EEI, complete the Student Contact Information Form; and
f) Ensure a copy of the Student Contact Information Form is placed on file at EEI.

4.2.2. **Phase 2: Response**

4.2.2.1. The staff member directly involved with the critical incident is to:

a) Ensure the physical safety of students and staff as a matter of urgency (i.e. lockdown or evacuation of premises);
b) Call emergency services as appropriate on 000;
c) Call the Critical Incident Coordinator (CIC) at EEI;
d) Refer directly to the Immediate Response Checklist for response action specific to the incident.

4.2.3. **Phase 3: Recovery**

4.2.3.1. The CIC at EEI is to:

a) Provide all those affected by the incident with access to factual information;
b) Contact the CEO at EEI;
c) Coordinate the de-briefing of those affected within 8 hours of the incident;
d) Monitor the need for counselling. Initiate and maintain contact with those affected by the incident;
e) Assess the need for on-going additional support from outside agencies.

4.2.4. **Phase 4: Review**

4.2.4.1. A Recovery and Response Plan to assist students affected by a critical incident will be reviewed annually by the Administration and Marketing Manager and the CEO or in the event of a critical incident, one-week post incident, 2 months post-incident and 6 months post-incident.

Meeting 1: The CIC and the CEO to meet within one week of incident.

Purpose:

- De-brief and update on outcomes.
- The Critical Incident Policy requires the CIC to complete a Critical Incident Report to build on cumulative experience of handling crises so that EEI can improve its crisis response. This report is to be completed at the initial meeting.
- Assess the need for legal advice.

Meeting 2: CIC and CEO to meet two months post-incident Purpose:

- Review of recovery phase. i.e. Assess need for ongoing counselling; provision of Memorials, resource management, involvement with coronial inquests etc.
- Re-assess legal position.

Meeting 3: CIC and CEO to meet six months post-incident

Purpose:

- Review EEI critical incident policy and procedures.

4.3. Risks and Prevention Checklist

4.3.1. Catastrophic event

4.3.1.1. Risk

a) Origin is unexpected or unanticipated and may occur at a local, state, national or global level.
b) Hazards include pandemic or infectious matter placing all staff and students of the institute at a serious health risk.
c) Impacts all physical facilities and operations of the institute.
d) May vary from discrete and short duration to protracted timeframes.

4.3.1.2. Preventative Measures

a) Adoption of all health and medical advice or directives from local, state or national health agencies.
b) Provide regular communication to all staff and students on measures adopted by the institute and arrange information and debrief sessions. Reaffirm that only communication from an approved institute source (CIC or Registrar) constitutes the institutes advice and information.
c) Other prevention activities may include reviewing and modifying work practices, improving physical security (such as sign-in procedures), adopting screening and other health checks, lockdown of campus, temporary closure or evacuation and continuous modification of operations in accordance with the manifestation of the catastrophic event.
d) A risk assessment is to be performed by the CEO and presented to Council for approval. Council to consider recovery options.
e) Providing reports to authorities as required.

4.3.2. Fire

4.3.2.1. Risk

a) Origin could be internal or external
b) Internal hazards - electrical equipment and connections, chemicals and other offices in the building
c) Student computer room poses the highest risk factor due to quantity of electrical devices and connections.

4.3.2.2. Preventive Measures

a) The building provided fire protection measures including fire alarms, smoke detectors, sprinkler system, fire extinguishers, building construction and floor plans to assist with evacuation.
b) All staff and students participate in the fire drills and practice evacuation procedures.
c) Regular inspection of fire extinguishers and smoke detectors.
d) Emergency electrician contact details are available from the Administration and Marketing

Manager.

4.3.3. **Water**

4.3.3.1. Risk

a) Origin could be internal such as leaking or damaged pluming.
b) Origin could be external such as leaks due to storm damage or flooding.

4.3.3.2. Preventive Measure

a) Regular inspection of the premises - in particular the computer room.
b) Any water leakage must be reported to the building manager.

4.3.4. **Criminal Behaviour**

4.3.4.1. Risk

a) Destructive or threatening behaviour by an individual or group such as: physical attack, bomb threat, theft, vandalism, or firearm incident, etc.

4.3.4.2. Preventive Measure

a) The buildings are alarmed outside operating hours.
b) Offices and facilities are kept locked outside operating hours.
c) All confidential information is physically or electronically secure.
d) Staff training.
e) Emergency contact detail for security staff and emergency services are posted by all staff phones and in student areas.

4.3.5. **Data / Information Security**

4.3.5.1. Risk

a) System failure.
b) Physical destruction of computer server and information storage areas.
c) Corruption or theft of data.
d) Electrical overload.

4.3.5.2. Preventive Measures

a) System back up
b) Scanning of vital hardcopy documents
c) Offsite document storage.

d) System security including: firewalls, password protection
e) Lockable storage areas and filing cabinets.
f) Use of quality databases.

4.3.6. Communication

Effective communication throughout the organisation is critical during a critical incident. The CIC is responsible for liaison and communication with all relevant persons and organisations.

4.3.7. Training

All staff will receive a copy of the Critical Incident Policy and WH&S training as part of their orientation. All staff and students will participate in regular emergency evacuation training.

4.4. Equipment and materials

All emergency equipment will regularly, checked, serviced and replaced when necessary. Sufficient equipment and material for effectively responding to recovering from emergencies will be available, including First Aid.

4.5. Useful Documentation

These are held by the CEO and ICT Manager

- The Organisational Chart with staff names and positions
- The Critical Incident Report
- Up to date staff contact details and the nominated critical incident coordinator
- Up to date student lists
- Emergency Services and Security contact details
- Supplier contact details
- Evacuation procedures
- Floor plans showing emergency exits
- Details of staff with First Aid training
- Insurance information
- ICT system specification
- Copies of maintenance agreements