Critical Incident Policy

1. Purpose

The Critical Incident Policy guides and protects the interests of staff and students and ensures that risks to KOI’s operations are managed appropriately. The policy is designed to ensure that KOI is prepared for critical incidents and has clear protocols to follow in what can potentially be distressing and upsetting circumstances.

This policy establishes the strategy for managing critical incidents and assigns responsibilities for its development, implementation, maintenance and review.

The Education Services for Overseas Students Act 2000 (ESOS Act) sets out the legal framework governing delivery of education to international students in Australia on a student visa. In particular, Standards 6.8-6.9 of the National Code of Practice for Providers of Education and Training to Overseas Students 2018 set out obligations for maintaining a safe environment and documentation of critical incidents and responses.

2. Scope

This policy applies to all KOI students, staff, contractors, partners and visitors, whether situated internally at the KOI or undertaking external work, who are involved in a critical incident.

3. Areas that can involve critical incidents

The following examples illustrate areas of risk where critical incidents may occur.

a) **Emergencies** (including fire, bomb threat)

b) **Unusual or bizarre behaviour** (including self harm, Interfering with class/activity)

c) **Workplace violence** (physical or sexual assault, threats, stalking, property damage)

   See the Prevention of Workplace Bullying and Harassment Policy and the Prevention of Sexual Assault and Sexual Harassment Policy

 d) **Critical injury or death** (workplace injuries accident, crime, self-harm)

 e) **Overseas travel and incidents** (terrorist act, medical emergency, severe weather)

   See the Travel Policy.

 f) **Civil disorder** (protests, demonstrations, riots, picket lines)

 g) **Communicable diseases** (eg HIV-Aids, Hepatitis B – E, epidemics and pandemics)

 h) **Media enquiries.** See the Media and Freedom of Expression Policy.

 i) **Information technology disruption** (data breaches, attacks, outages, viruses)

4. General response procedures (for all types of critical incidents)

KOI maintains a system of emergency preparedness and response consistent with Australian Standard 3745-2010 and its associated guidelines.

KOI has a hierarchy of control that includes:

- Work Health and Safety Officer
- IT Manager (for responding to information technology disruptions)
- Floor or Area Wardens
The Work Health and Safety Officer will provide reports about all critical incidents and response strategies at KOI to the CEO and Dean.

KOI will maintain a comprehensive emergency plan and training for all staff must appropriate to their level of appointment and responsibility.

Initial action on detection/report
1. Ensure the safety of all persons. If emergency services are required arrange them immediately.
2. Report urgently any potential emergency to the nearest Warden (lists and contact details are provided at all emergency exits).
3. Note the exact location and brief circumstances to advise the Warden including any action taken such as 000 call for emergency services (Incident Report Form must be subsequently submitted within 24 hours).
4. Inform the CEO and Dean immediately.
5. If available, review the security surveillance system to ascertain whether the incident was captured on the system.
6. If an international student is involved, notify Student Services. The state office of DHA must be notified, an entry made on PRISMS, the relevant Consulate informed and the student accommodation provider advised.
7. If there are casualties, next-of-kin should be informed by or on authority of CEO and Dean. Personal effects of casualties listed, witnessed and secured.

Communication
1. Other than communication with the emergency services, no communication is to occur outside of KOI. Media enquiries are to be referred to the CEO and Dean.
2. The duty officer will maintain a communication log throughout detailing time, activity and follow-up requirements.
3. CEO and Dean or delegate to be updated regularly so as to provide an accurate media release (if relevant) and current appraisal.

Post-incident action
1. Incident notification for relevant persons (staff, students and others) only after legal advice and consent from the police (if relevant).
2. Staff and students to be offered counselling – interpreters may also be required.
3. KOI administrative processes to be completed including Incident Report Form.
4. Personal effects of casualty provided to next-of-kin with detailed and signed receipt if relevant (Receipt of Goods)

5. Roles and responsibilities
The CEO and Dean is responsible for overseeing the application of this policy within KOI, including review of relevant incident reports and other documentation, and for reporting on critical incidents and responses to the Council.

The Work Health and Safety Officer is responsible for implementing all functions of the emergency control system, arranging training and awareness sessions and preparing reports on all critical incidents.

All Managers are responsible for ensuring that staff in their area of operation are aware of this policy and that this policy is adhered to.

Managers/Supervisors have planning responsibilities:
   a) Identifying potential critical incident circumstances, assessing and controlling of critical incident risks effectively
   b) Implementing, monitoring and maintaining risk control measures for critical or potential critical incidents in their areas of responsibility
   c) Regularly monitoring the effectiveness of critical incident risk control measures and rectifying any deviations from procedures
   d) Consulting with staff and others with competence in the area on critical incident practices or any proposed changes
   e) Ensuring staff are trained and competent in how to behave during a critical incident
f) Ensuring there are appropriate post-incident strategies in place to minimise the impact of a critical incident.

Managers/Supervisors have responsibilities during the response phase:
- a) Confirming the accuracy and full extent of a reported incident and reporting to designated personnel
- b) Implementing relevant procedure(s) within their area of responsibility. This includes communication with key stakeholders
- c) Ensuring any follow-up action occurs at the earliest possible time
- d) Contributing to a post-incident debrief and critical review of KOI responses.

Staff are responsible for complying with this policy.

Staff have responsibilities not to place themselves or others at risk of injury. Staff should:
- a) Report to manager/supervisor or the most convenient Warden any critical or potentially critical incident and any significant symptoms which may have resulted from a critical incident
- b) Assist manager/supervisor/Wardens with the identification of hazards, the assessment of risks and implementation of risk control measures related to critical incidents
- c) Follow established critical incident (emergency) procedures
- d) Provide immediate support as appropriate for anyone involved in a critical incident (emergency)
- e) Access support mechanisms where there has been exposure to a critical incident (emergency).

6. Additional guidance

Unusual or bizarre behaviour

Incidents involving unusual or bizarre behaviour must be formally managed in a sensitive and strategic way.

The following are behaviour signs to look for:
- Inability to follow instructions
- Severe agitation or distress
- Confusion
- Suspiciousness
- Threats of self-harm or harm to others.

In addition to the general response procedures:
- If safe to do so, approach the person and discuss concerns.
- Contact the Counsellor to check if other people are affected by the incident and take appropriate action, eg debriefing, grief counselling.
- Consider if the issue should be treated pursuant to discipline procedures.

Workplace violence

Where a physical assault has occurred immediately contact police and consider preservation of evidence. Notification of the incident for relevant persons (staff, students and others) should occur only after legal advice and consent from the police (if relevant).

Victims of domestic violence should advise the appropriate person at KOI (for example, their teacher, supervisor, HR manager, or Counsellor), especially where an intervention order or similar is in existence. Where possible, KOI will seek to minimise the risk of a breach whilst the victim is in or around KOI property.

Critical injury or death

Incidents involving critical injury or the death of a student, staff member or other person associated with KOI in any way must be formally managed at the highest levels of KOI.

Where critical injury or sudden death is detected, the scene must be preserved as per crime scene management strategies and the emergency services called on 000.
Where it is a critical injury emergency, first aid procedures must be implemented pending the arrival of the emergency services (safety overrides scene preservation).

If death, it must be confirmed as soon as possible (may also include mortuary identification). If critical injury, hospital details to be noted.

If death, liaise with next-of-kin regarding funeral arrangements and, where relevant, transfer of body overseas. May also involve religious group interactions.

Incident notification for relevant persons (staff, students and others) only after legal advice and consent from the Coroner and police (if relevant);

Staff and students to be offered grief counselling or counsellor present for the notification – interpreters may also be required;

**Civil disorder**

Staff and students at campuses and colleges may become accidental victims of acts involving civil disorder. Avoiding or minimising this risk generally involves staying away from gatherings no matter how peaceful they may appear at the outset.

Incidents of civil disorder at college/campuses can result in serious damage to the organisation and potential harm to staff and students. They must be formally and strategically managed.

The safety of all staff, students and others present is paramount therefore those presenting a threat should be isolated where possible. Call relevant emergency services immediately. Staff and students should not put themselves or others in danger.

Incident notification for relevant persons (staff, students and others) only after legal advice and consent from the CEO and Dean. Staff and students to be offered counselling as required. Arrange for repair of damaged property as soon as possible and secure KOI premises.

**Communicable disease**

*Communicable disease* is any disease or infection caused by a viral, bacterial, fungal, parasitic or other agent that is likely to result in death or a life-threatening or debilitating illness.

A communicable disease may be transmitted in a human population by direct physical or environmental contact between an infected and non-infected person, contact with infected organic material, or contact with an animal, insect or parasite that is host to an infectious organism.

Communicable diseases must be reported to the relevant health authority within the jurisdiction.

Occupational health and safety legislation in NSW requires employers to ensure the occupational health and safety of workers against communicable diseases. Employers are expected to conduct a risk assessment to identify and assessment of potential hazards, including biological hazards, and the subsequent elimination or control of those risks.

A worker who contracts a life threatening or debilitating communicable disease has a duty to take reasonable care for the health and safety of other employees and other persons at their workplace. They must advise the CEO and Dean or nominee of their condition. Notification may be via a medical certificate from the worker’s treating doctor. If a worker fails to take this action without reasonable cause, they may be in breach of WHS and health legislation.

If the nature of the disease is known to the CEO and Dean, he must ensure that all workers and other persons who have contact with the person in question are informed of the nature of the disease. The CEO and Dean has an obligation to protect the worker’s privacy in such circumstances and ensure that the worker is not discriminated against if information on the communicable disease becomes known.
Health and Hygiene Guidelines are provided by DHA and apply to hepatitis, HIV/AIDS, tuberculosis or similar infectious diseases. For a highly contagious disease personnel must follow Department of Health and Ageing protocols and any other protocols issued from time to time.

**Procedures**

- **a)** Advise and/or post warnings in the premises to alert workers, clients/contractors, students or other persons who have traveled to and from a local or international source of infection:
  - That any physical contact with the workforce is to be avoided to prevent any risk of cross infection
  - A time period in excess of the known incubation period for the disease or time period where there has been a potential cross infection

- **b)** Workers, students or clients who might be infected should avoid attendance in the workplace or exposure to other workers until the relevant period has passed unless they produce a medical certificate that states they are not an infection risk to others – students should be given home tasks so their studies are not adversely affected

- **c)** If there is a conflict between a medical certificate and the instructions of the health authority, the health authority takes priority

- **d)** Where there has been contamination or exposure, consideration must be made to having infected persons work from home for the duration of the risk, relocation to another workplace, taking leave or closing the workplace. Where closure occurs, consideration should be made to full or part closure, quarantine or decontamination, or such other action deemed appropriate to eliminate or control the communicable disease.

**Information Technology Disruption**

A data breach is a breach of personal data security that is likely to result in serious harm to any of the individuals to whom the data relates. If it is not possible to prevent the likely risk of serious harm with remedial action, a decision must be made to notify the Australian Information Commissioner. This decision is made by the CEO and Dean on the advice of the IT Manager. The IT Manager must notify the affected individuals that the notification of a potential eligible data breach has been lodged with the Australian Information Commissioner and inform them of the contents.

Where possible the IT Manager must initiate steps to reduce any potential harm to individuals. This may involve taking action to recover lost data before it is accessed or changing access controls on compromised accounts before unauthorised transactions can occur. If remedial action is successful in making serious harm to individuals no longer likely, then notification to the Australian Information Commissioner is not mandatory.

**Adapted from a document developed by the Australian Institute of Public Safety**

**Document control**

<table>
<thead>
<tr>
<th>Policy title</th>
<th>Critical Incident Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy owner</td>
<td>CEO and Dean</td>
</tr>
<tr>
<td>Policy approver</td>
<td>Council</td>
</tr>
<tr>
<td>Version date</td>
<td>6 November 2019</td>
</tr>
<tr>
<td>Date approved</td>
<td>5 November 2019</td>
</tr>
<tr>
<td>Date of next review</td>
<td>1 November 2023</td>
</tr>
</tbody>
</table>

***************END OF POLICY***************