Guide to responding to critical online incidents

Creating safer online environments

Disclaimer: This material is general in nature. It is made available on the understanding that the Commonwealth is not engaged in rendering professional advice. Before relying on the material in any matter, you should carefully evaluate its accuracy, currency, completeness and relevance for your purposes and should obtain any appropriate professional advice relevant to your circumstances. The Commonwealth does not guarantee and accepts no legal liability whatsoever arising from or connected to, the accuracy, reliability, currency or completeness of any material contained in this resource or on any linked site. References to other organisations or websites are inserted for convenience and do not constitute endorsement.

Australian Government

eSafety Commissioner

eSafety.gov.au

Why has this guide been produced?

A critical online incident is a specific event, or the threat of an event, which causes extreme stress, fear or harm. A critical online incident can occur in any school, and it can disrupt student learning and impact student and staff mental health and wellbeing. A critical online incident requires immediate intervention and response.

This guide provides support and advice to Australian schools to respond confidently and effectively to critical online incidents, including serious cyberbullying, image-based abuse, and exposure to harmful and/or illegal content. Online safety policies and procedures should align with relevant legislation, as well as school and/or education sector policies and procedures.

Important Note

Regardless of when or where an incident has occurred, or whether the incident meets the threshold of 'critical' if a student is distressed and needs support, their wellbeing, rights and best interests should guide your response.

Schools should have a designated person or team of people responsible for online incidents. All members of staff (including non-teaching) need training to recognise, respond to, or refer, serious online safety incidents. This can be covered in professional learning and school policy.

1. Understand and assess

If a staff member becomes aware of a critical online safety incident at school, or a student discloses an online incident that is causing significant harm or has the potential to cause significant harm, it should be investigated as soon as possible.

If the student/s is in immediate danger, call police on Triple Zero (000).

The wellbeing and protection of the student/s involved (including the target/s, instigator/s, and upstanders/bystander/s) should always be the primary concern – follow your school and/or education sector's safeguarding and child protection policies and procedures.

The student/s affected may experience fear, anxiety, anger or distress. It can be helpful to involve a staff member who the student nominates as someone they trust so they are supported during the disclosure and reporting process.

Support students and staff. Use a trauma-informed approach that prioritises safety, builds and maintains trust, respects autonomy, and reduces the risk of re-traumatising those affected.

When taking a report, remain calm, reassuring and non-judgemental. Do not say or do anything to blame or shame the student/s involved. It is important that responses are child-focused and age-appropriate.

Speak with the affected student/s as soon as possible and try to find out:

- Who is involved, how many and their ages if known?
- What has happened (bullying, image-based abuse, engaging with illegal and/or restricted content)?
- How has it occurred (sharing or posting of content, photos, videos, messages? On what specific device, platform, service, or app)?
- If content has been shared, how widely has it been shared and with whom?
- When did it happen (during school time? after school hours? when did it start, when did it stop, is it ongoing, how often has it happened)?
- Where did it happen (on a school or personal device? Is it occurring at school, at home or somewhere else)?
- What are the circumstances surrounding the incident (is it part of a wider situation that is occurring online or face-to-face)?
- Who else is aware of the issue (other students, parents/carers, staff, the media)?
- Is the incident likely to be repeated?
- What other vulnerabilities do those affected have that should be considered in the response?
- Has a report already been made to police?
- Has a report already been made to the platform, service or app?
- Has a report already been made to eSafety via the 'Report abuse' portal?

2. Collect and preserve evidence

Evidence can include webpage addresses (URLs), account names/profiles and usernames.

Collect evidence to provide to police and eSafety but avoid unnecessary exposure to and storage of explicit material. Make a written description and note where it is located.

- For non-explicit material, where possible, take screenshots and record URLs, account or profile names and usernames and other information about where the material is located and/or where the harm has occurred.
- For explicit material (for example, intimate images or videos including deepfakes or illegal and/or restricted content), do not take screenshots, view, or share the material — refer to eSafety's Respond 3A - Guide to responding to image-based abuse, including sexual extortion and Respond 3B – Guide to responding to image-based abuse involving AI deepfakes.

It may be necessary to temporarily remove and secure devices if this is permitted by school and/or sector policies and procedures. Refer to eSafety's Respond 3A - Guide to responding to image-based abuse, including sexual extortion and Respond 3B – Guide to responding to image-based abuse involving AI deepfakes for further information about dealing with devices during critical incidents. Please note, this advice is relevant even if the incident does not involve image-based abuse.

3. Manage the response

Inform the principal and determine a designated lead from the school's leadership team to coordinate the response.

Consult with relevant centralised education sector support (for example, critical incident response or student wellbeing team) where appropriate.

Do not formally interview students (particularly the student/s responsible) or ask for written statements. This is not the role of the school. Should police become involved, they may do this as part of their investigations, and students and/or their parents/carers may wish to seek legal advice.

Focus on providing support for all students and involve them in decision-making.

Work with the student/s involved to understand the circumstances surrounding an incident, noting that it might be part of a broader situation occurring online or face-to-face.

Additional support may be required, and the response should be tailored for the specific incident type and focused on student safety and wellbeing. Critical incidents may involve unlawful behaviour that requires a report to police or triggers mandatory reporting obligations.

Inform and involve parents/carers as soon as possible so that the school and the family can work together to respond to the incident, unless there is a good reason not to. For example, if it puts the student at further risk or hampers a possible police investigation. Consider giving the young person the opportunity to tell their parents/carers themselves.

Follow your school and/or education sector's safeguarding and child protection policies and procedures for engaging with students' families.

Student's families should be kept appropriately informed about the actions being taken by the school to address the situation and ensure their child's safety and wellbeing.

Discuss the most appropriate course of action with the relevant school and/or sector advisors, police and child protection authorities as required.

Assess whether school-wide communication is appropriate.

4. Report harmful content and prevent further contact

eSafety has four reporting schemes that are important to know about. eSafety can investigate cyberbullying of children, adult cyber abuse, image-based abuse (sharing, or threatening to share, intimate images without the consent of the person shown) and illegal and restricted content. Harmful content can be reported using eSafety's 'Report abuse' portal.

School staff should advise or assist the student to report harmful content to eSafety and, once all available evidence is collected, encourage all students to delete the content from their devices.

If a student refuses to delete the content from their device, consider confiscating the device in line with the relevant education department or sector policy. Escalating the issue to parents/carers or the police may be required.

If an online service or platform fails to remove reported content, and the content constitutes serious cyberbullying, students, their parent/carer or an authorised adult can make a complaint to eSafety. Student permission is required to lodge a complaint on their behalf. This can be a verbal or written agreement, noting that verbal approval should be recorded. Staff and students might consider lodging the complaint form together.

eSafety has the authority to direct online services or platforms to remove seriously harmful content that has been sent to an Australian or posted or shared about them.

Prevent further contact with the person who is causing harm by using in-app functions to ignore, mute or block them. It is also important to check privacy settings.

It is important to note that eSafety may assess that, while the content may be upsetting or hurtful to the person targeted, the content may not reach the Online Safety Act's threshold for being seriously damaging to the person targeted. In these cases, eSafety will be unable to seek removal of content online.

While eSafety may not be able to help to get the content removed, we can provide advice and support to minimise the impact on the person targeted.

5. Resolve the conflict

A school's response should be proportionate to the nature, severity and impact of an incident, and in the best interests of the student/s involved.

Staff should follow their school and/or sector behaviour management policies when responding to misconduct, focus on restoring relationships and work with the students and parents/carers involved to resolve the issue.

If appropriate, staff could invite resolution suggestions from the student/s involved. A skilled mediator or facilitator may be required.

The aim is for the student/s responsible for online misconduct to take responsibility for their actions, apologise and make amends, and understand not to repeat the behaviour. Focus on restoring relationships and ensuring all students feel safe and supported.

It is important that staff follow up with parents/carers to discuss the actions the school has taken to resolve the issue and strategies to follow if the behaviour is repeated.

Depending on the type of incident and the wellbeing of the students involved, it may be helpful to involve school counsellors or engage external support services. Your school and/or education sector may also offer tailored support.

Teach online safety education using a whole school approach to equip students with knowledge and, skills for respectful online behaviour.

Assess whether school-wide communication is appropriate and what type of longer-term intervention is required, such as engaging external providers (for example, Trusted eSafety Providers).

School staff can reinforce, model, and promote acceptable use of online tools.

6. Record and reflect

Record incident details, response, and actions taken in the school incident management system or equivalent in accordance with school and/or education sector protocols. Recording incidents supports further monitoring and ensures a robust approach in assessing the school's online environment. Incident records may also be used if police or legal action is required. In these circumstances, schools, students and their parents/carers may need to seek legal advice.

Complete eSafety's Respond 8 - Post-incident checklist to help evaluate how effective the response was, and to identify areas for improvement. A review of existing policies and procedures should be included.

Debrief with staff, students and parents/carers where appropriate so they understand the steps taken to resolve the issue and the strategies that will be used to reduce the risk of the behaviour happening again or if it continues.

7. Monitor the situation

Schedule regular follow-ups with students to check on their wellbeing, cultivate pro-social behaviour, and build a positive school climate with healthy student-teacher relationships.

Monitor student behaviour for signs of recurrence and intervene early.

If issues continue, it is important that the repeated behaviour is addressed proactively with the students involved and across the school.

Adjust plans if necessary.

Review processes to identify how incident responses can be strengthened.