Guide to assessing online safety 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?

This guide provides school staff with a resource for assessing online safety incidents. It lists key considerations, the types of online behaviours that are likely to require a response and explains eSafety's reporting schemes.

A note about online incidents involving social media: No matter how old your students are, if they experience an online incident, they should feel free to ask you for help – even if they are under 16 and it has happened on an age-restricted social media platform or service. Remember, if an under-16 has an account on an age-restricted social media platform they are not breaking the law. It's only the platforms and services themselves that face penalties if they fail to take reasonable steps to stop under-16s creating or having accounts.

This guide should be read alongside school and/or education sector policies and procedures, especially those relating to student behaviour, code of conduct, acceptable use, and child protection.

Using this resource

Online safety incidents can lie on a continuum from mild to critical. It can be difficult to assess their seriousness and potential impact because incident features can differ widely.

When deciding how to respond, some key considerations include student characteristics such as risk and protective factors, the type of incident, who was involved and how many, its frequency and duration, and the likelihood of stopping the harm.

Use caution and seek guidance from trusted school and/or education sector advisors, policies and procedures.

More detailed response guidance is provided in Respond 2 – Quick reference guides for responding to online safety incidents and Respond 3 – Guide to responding to critical online safety incidents.

Key considerations

It can be difficult to predict the seriousness of an online safety incident and the impact it may have on those involved because this will vary according to a range of factors.

All online incidents need to be taken seriously and responded to, in line with your duty of care to students and staff.

As a priority, check your school and/or education sector policies and procedures for reporting obligations – you may need to report online safety incidents to school and/or education sector critical incident units, local police, child protection authorities, reportable conduct schemes, and/or the eSafety Commissioner.

Here are some key considerations for assessing online safety incidents:

- **Student characteristics**. Their strengths and vulnerabilities, including their age and developmental stage, their coping strategies, family circumstances, peer group, and available supports.

  Consider the needs of students involved including those with disability, First Nations students, LGBTQI+ students, those from diverse linguistic and cultural backgrounds, students experiencing family separation and/or divorce, those in out-of-home care and others who may be vulnerable and susceptible to online harms.
- **The type of incident**. What has happened, the words, symbols and expressions used, and the specific content created or shared including whether it involved coercion, intimidation or force, and if threats have been made.
- **Who is involved and how many**. The relationship(s) among those involved – if the incident is contained between two students, or a specific student network group, or has been shared far and wide. Consider the dynamic nature of relationships: for example, targets and bystanders can also become instigators, and instigators and bystanders can also become targets.
- **The platform or service involved**. The type of platform or service involved, if and where the content has been stored or shared, the number of times it has been shared or viewed, where, and with whom.
- **The frequency and duration of the incident/s**. If the incident has happened only once, occasionally, or many times, and over what period.
- **The likelihood of harm stopping**. If the instigator has agreed to stop, if they have continued after they have been asked to stop, if they are continuing and unlikely to stop.
- **Legality/illegality**. Some online safety incidents may involve unlawful or criminal behaviour such as child sexual abuse and/or exploitation. Instigators may be known or unknown. If you believe a crime has occurred, it should be reported directly to police. eSafety is an independent regulator focused on online safety and cannot investigate criminal offences. eSafety can help with harmful online content and abuse but some incidents are best reported to police.
- **Disclosure**. If a direct or indirect disclosure of harm has occurred. If they have told someone previously and not been believed or had no action taken. Use disclosure response strategies learned in child protection training – these can apply to online safety incidents as well.

Online behaviours

By learning about students' online behaviour school staff can be better equipped to respond effectively to online incidents. Below are some examples of behaviours that require intervention and response. A description of the behaviour is provided along with links to eSafety resources.

The table below is intended as a guide only and it is not an exhaustive list. Remember, the individual circumstances of online incidents will vary and incidents that appear similar may differ in their impact and seriousness. There should always be a response to student behaviour, but the response will vary.

Behaviour	Description
Teasing, name calling, put downs	Name calling, making fun, or swearing at or about someone. Using memes (pictures or videos with accompanying text) that are designed to make fun of someone, disguised as a joke. Schools can easily manage responses to this type of behaviour, but if there's repeated incidents or the content is shared widely it can become seriously harmful for the person targeted and reporting to the platform or service may be required. ℹ **More information:** Cyberbullying fact sheet and Spotlight on cyberbullying, Respond 2 – Quick reference guides for responding to online safety incidents. See also Standard 6 from the Australian Government's Anti-Bullying Rapid Review.
Excluding, blacklisting, cancelling	Leaving someone out by deleting them from group chats, excluding them from online groups, games or other activities, digitally altering photos to deliberately exclude them from a group. Encouraging others to join in freezing someone out. ℹ **More information:** Cyberbullying fact sheet and Spotlight on cyberbullying, Respond 2 – Quick reference guides for responding to online safety incidents.
Fake accounts, impersonation, catfishing	Creating fake social media profiles to damage someone's reputation, misrepresent them, disrupt their friendships or relationships, intimidate or harass them. ℹ **More information:** Cyberbullying fact sheet, Coercive control: information sheet, Spotlight on cyberbullying, Respond 2 – Quick reference guides for responding to online safety incidents.
Student and/or staff ratings	Creating or following accounts or sharable documents that feature ratings, polling, or other commentary on student and/or staff attractiveness, appearance, or behaviour. ℹ **More information:** The eSafety Guide, Respond 2 – Quick reference guides for responding to online safety incidents.

Viral online trends	Viral trends that encourage users to copy a stunt or behaviour. These can be motivational and fun (for example dance challenges) annoying (the ‘6-7’ meme) or harmful when they lean towards incitement to violence or self-harm. ℹ **More information:** Dangerous or damaging online challenges are never funny, Respond 2 – Quick reference guides for responding to online safety incidents.
Fight videos and other violence	Creating and following accounts that feature fight videos, or other depictions of violence such as students engaging in bullying or harassment. ℹ **More information:** Dealing with fight videos, Respond 2 – Quick reference guides for responding to online safety incidents.
Unwanted contact and grooming	Contacting a student online to send them uninvited messages, persuade them to do risky things like share personal information (including images or videos), buy things, or join a new chat or group. They might try flattery, pretend to be a friend, or make gradually more threatening requests. This may be a warning sign for child sexual abuse or sexual extortion. It could also be an attempt to recruit the student into groups sharing harmful ideas and behaviours. ℹ **More information:** Unwanted contact and grooming: factsheet, Respond 2 – Quick reference guides for responding to online safety incidents. See also Step Together Resources for Teachers - Quick reference guide.
Online hate	Hateful posts about a person or a group of people based on their race, religion, ethnicity, gender, sexual orientation or disability. When online hate is targeted towards a specific person, it's considered to be cyberbullying. ℹ **More information:** Report online harm. Respond 2 – Quick reference guides for responding to online safety incidents, Respond 3 – Guide to responding to critical online safety incidents. See also Step Together Resources for Teachers - Quick reference guide.
Harmful use of AI chatbot companions	AI companions are readily available. They can share harmful content, distort reality and give advice that is dangerous. In addition, the chatbots are often designed to encourage ongoing interaction, which can feel ‘addictive’ and lead to overuse and even dependency. ℹ **More information:** AI companions: information sheet, Respond 2 – Quick reference guides for responding to online safety incidents, Respond 3 – Guide to responding to critical online safety incidents.

Incitement to self-harm or suicide	Encouraging or pressuring a student to self-harm or consider suicide. When directed to a specific person, it's considered to be cyberbullying. **Note:** if you become aware that a student has been posting online or searching for or receiving information about suicide or self-harm online, refer to your school's duty of care policy and seek advice from local police and support services. Orygen's #chatsafe guidelines and headspace may provide additional support. ℹ **More information:** What you can report to eSafety, Respond 3 – Guide to responding to critical online safety incidents.
Threats of physical harm	Threatening to physically hurt someone — sending seriously threatening messages, sharing fight videos with threats of retaliation or posting codified suggestions that serious harm will be inflicted. When directed to a specific person, it may be considered cyberbullying. Depending on the circumstances it may also be a type of coercive control. ℹ **More information:** What you can report to eSafety, Respond 3 – Guide to responding to critical online safety incidents.
Nude images have been shared	Sharing intimate images or videos without the consent of the person in the image is image-based abuse. It is illegal. Intimate images or videos are those that show someone: • nude or partly naked – such as a naked selfie or a topless photo if they identify as female or non-binary • genitals, bottom or breasts – even if they have underwear on (this includes upskirt shots) • during a private activity – such as undressing, using the toilet, showering, having a bath or getting sexual • without clothing of religious or cultural significance, if they would normally wear it in public (such as a hijab or turban). ℹ **More information:** Report abuse; Respond 3A – Guide to responding to image-based abuse, including sexual extortion, Respond 3B – guide to responding to image-based abuse involving AI deepfakes
Is being blackmailed or threatened about their nudes	Blackmailing or threatening to share a student's nude image or video unless they give in to their demands is a type of image-based abuse. It is illegal. It is sexual extortion. ℹ **More information:** Report abuse; Respond 3A – Guide to responding to image-based abuse, including sexual extortion, Respond 3B – guide to responding to image-based abuse involving AI deepfakes

Creation of deepfake images or videos of students or staff	A deepfake is a digital photo, video or sound file of a real person with an extremely realistic but false depiction of them doing or saying something that they did not actually do or say. Deepfakes can be created from everyday images like class photos. ℹ **More information:** Report abuse; Respond 3B – guide to responding to image-based abuse involving AI deepfakes, Respond 3A – Guide to responding to image-based abuse, including sexual extortion.
Exposure to disturbing content online	Students have been exposed to content that is disturbing or distressing because it shows offensive material, a seriously violent event or pro-terror content. Pro-terror content may be illegal. ℹ **More information:** Inappropriate content: factsheet, Report abuse.

Responding

Recalling that online safety incidents can lie on a continuum from mild to critical, it is likely that many incidents will be manageable at the school level with support and monitoring from school staff. Follow your school and/or education sector policies, procedures, and processes, and refer to the Toolkit for schools for advice.

- Respond 2 – Quick reference guides for responding to online safety incidents provides a provides a framework for thinking about online safety incidents on the continuum from mild to critical. It offers advice on potential responses corresponding to points along the continuum.
- Respond 3 – Guide to responding to critical online safety incidents provides support for incidents at the critical end of the continuum that cause extreme stress, fear or harm.

It is important to know that eSafety has four reporting schemes and that reports can be made online:

1. **Child cyberbullying**
2. **Image-based abuse**
3. **Illegal and restricted online content**
4. **Adult cyber abuse**

eSafety also accepts complaints about online services that are not complying with online safety codes and standards. eSafety uses the information provided in complaints to identify failure to comply with online safety codes and standards designed to keep Australians safer online.