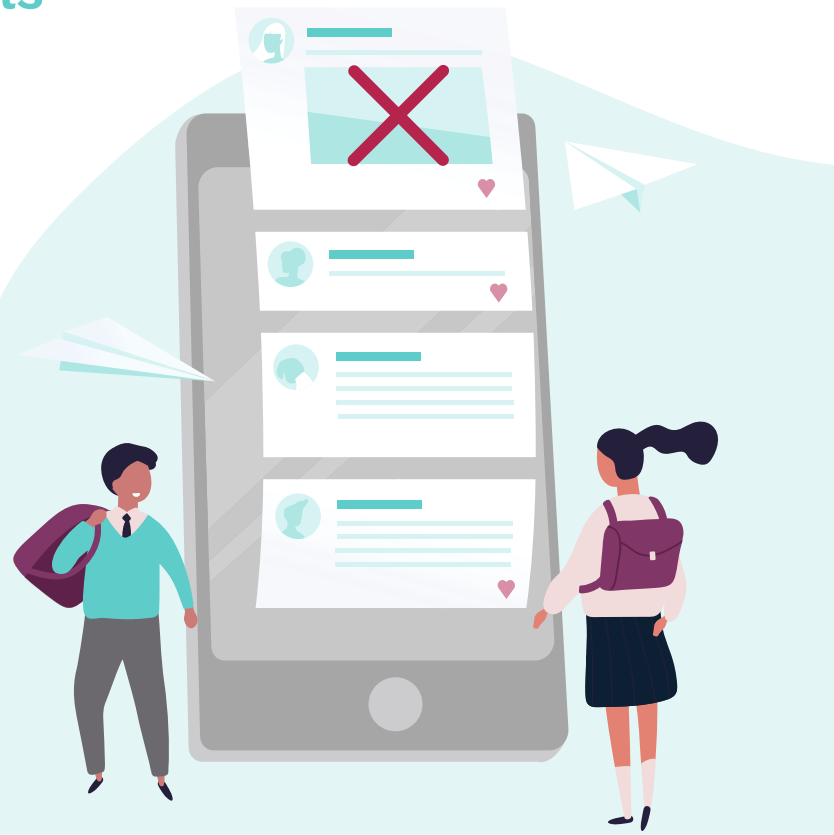
Guide to responding to image-based abuse, including sexual extortion

eSafety Toolkit for Schools

Creating safer online environments



Why has this guide been produced?

This guide provides support and advice to help school leaders respond effectively to incidents of image-based abuse. This guide should be read alongside safeguarding and child protection legislation, policies and procedures relevant to your school and/or education sector.

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 particular 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.

What is image-based abuse?

Image-based abuse is where someone shares, or threatens to share, an intimate image or video of a person without their consent. The image or video can be real, digitally altered or a deepfake created using artificial intelligence (AI) tools and apps. Image-based abuse can also involve sexual extortion – for example, where a student has been tricked into sending a nude image or video and the receiver threatens to share it online or with contacts unless the student gives in to their demands.

The creation and/or sharing of intimate images or videos by young people is seldom straight forward. It is complex and requires sensitive treatment. This is true whether the image or video is real, digitally altered or a deepfake created using an artificial intelligence (AI) tool or app.

What are intimate images?

An image or video is 'intimate' if it shows, or appears to show:

- **a person nude or partly naked –** such as a naked selfie or a topless photo (if they identify as female, transgender, or intersex)
- **a person's genitals or bottom –** even if they have underwear on (this includes upskirt shots)
- **a person doing a private activity –** such as using the toilet, showering, having a bath or getting sexual
- **a person without clothing of religious or cultural significance**, if they normally wear it in public (such as a hijab or turban).

The circumstances surrounding the image or video must be such that an ordinary reasonable person would reasonably expect to be afforded privacy.

Staff professional learning

It is recommended that schools have a designated person responsible for responding to and reporting online incidents of image-based abuse, including when they involve sexual extortion or deepfakes. Ideally, this should be a designated member of the school leadership team such as a principal or deputy principal.

All members of staff (including non-teaching staff) can be trained to recognise, respond and report incidents involving students and image-based abuse. In addition to education sector-specific professional learning, eSafety's free **teacher professional learning** can support educators and others who work with students.

Regardless of a person's role in a school, if they become aware of an incident, it should be reported to the school Principal. You will need to adhere to mandatory reporting obligations and seek further advice from critical incident and/or student protection teams in your school and/or education sector.

Managing incidents

eSafety promotes a collaborative approach to managing critical online incidents like image-based abuse, including incidents involving deepfakes or sexual extortion.

The role of school leaders

You must act as soon as you become aware of an incident involving student/s and/or staff at your school.

For example, when:

- you find out that a real, digitally altered or deepfake intimate image or video of a student attending your school has been shared on an online platform, or via email, messaging app or text
- a student discloses this has happened to them
- a student discloses they have seen something created or sent by others
- a staff member discloses this has happened to them or a colleague.

Ensure you:

- find out all relevant information from school staff who were alerted to the incident or brought it to your attention
- do not share information about the incident with other staff members
- record, in writing, details of the incident and the actions taken in response
- go to the eSafety website and become familiar with the **'Report abuse' portal** which appears as a red button on the **eSafety homepage**.

Supporting students and staff members

The wellbeing and protection of the students and/or staff involved (including the victim, alleged offender and witnesses) should always be the primary concern – follow your school and/or education sector's safeguarding and child protection policies and procedures.

The student/s and or staff affected may be experiencing fear, anxiety, anger, shame, helplessness and hopelessness. 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 members using a trauma-informed approach that prioritises safety, builds and maintains trust, respects autonomy, and reduces the risk of re-traumatising those affected.

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

Talk with the affected student/s and staff member/s as soon as possible and collect information about:

- who is involved
- if those involved are at immediate risk
- if it's an image or video
- if it's on a school or personal device
- any steps the student or staff member has taken to manage the situation so far
- the names of the platform/s on which the material has been shared, with whom and how widely
- the account names, display names and/or URLs from which the material has been shared (see 'Collecting evidence' in this guide)
- whether an adult (someone 18 or older) is involved (for example in grooming, coercing, or blackmailing the student)
- any specific vulnerabilities the student or staff member has
- how the student is feeling at the time and what would help them to feel safe.

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.

Communicating with parents/carers

Inform and involve parents/carers as soon as possible, 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.

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

Steps to report

If someone shares or threatens to share a nude or sexual image or video of a student or staff member, follow the same approach for real, digitally altered or deepfake content. It is essential that the student/s impacted is supported in a trauma-informed way that promotes their sense of agency and involvement in decision-making.

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

This is eSafety's advice for **image-based abuse (except where blackmail is involved)**:

- **Collect evidence** to provide to police and/or eSafety – see details on the next page.
- **Report to local police** – they have powers to seize devices and conduct interviews and can advise you on whether their response is required. (Follow your school and/or education sector guidelines for reporting to police and child protection authorities.)
- **Obtain a job or event number** from the police if possible. Record it in writing, along with details about the officer you reported the incident to and the date and time.
- **Notify eSafety** using the eSafety **Report Abuse portal**, including details about any threats that have been made to share (more) images or videos.

Encourage those responsible to follow eSafety's advice for stopping the image or video spreading: **What to do if you shared someone's intimate image or video**.

In all image-based abuse incidents remain calm, reassuring and non-judgemental. Do not say or do anything to blame or shame the students involved. It is important that responses are age-appropriate, child-focused and avoid apportioning blame.

Engage additional support such as counselling and consider if there is a concern about risk of harm from others or self-harm. Young people can feel re-victimised each time the content is shared or viewed and may need ongoing support, beyond the immediate response period. If the student is presenting as suicidal or self-harming, consider notifying their parents/carers, implement child protection reporting obligations and refer the student to appropriate support services.

Remember that it is misleading to assume that deepfake or digitally altered content causes no harm or is victimless. This minimises the serious impacts such content can have on those targeted.

Further information can be found in **RESPOND 3A Guide to responding to image-based abuse involving AI deepfakes**.

Specific considerations for sexual extortion

If a student is being blackmailed for money or more intimate content, this is sexual extortion (sometimes known as 'sextortion'). It is a form of image-based abuse that requires a different response if the victim is under 18.

The school (and/or parents/carers) should follow these steps:

- Prioritise the immediate safety and wellbeing of all individuals involved.
- Advise the student to stop all contact with the blackmailer.
- Advise them NOT to pay the blackmailer or give them more money or intimate content.
- Report what is happening to the **Australian Centre to Counter Child Exploitation**.
- Understand it is not the fault of the student (even if they shared intimate content in the first place).

Collecting evidence

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

When dealing with intimate images or videos, remember these points:

- You do not need to view the image or video yourself and should avoid doing so. You will likely already have enough information about the material and who it depicts.
- Note details about the nature of the material, the specific platforms and/or other services on which it appears, and times and dates of events. Also make detailed notes about the handling and storage of devices that hold evidence, to support the police chain of custody.
- Do not copy, print, delete or further share the material as it may be unlawful to do so, leave this to the police if they become involved – they are the experts.
- Do not, under any circumstances, photograph, screenshot or send the image or video to yourself for evidence or have someone else do this for you.

Dealing with device/s

Here are some steps to consider when dealing with any devices involved:

- Temporarily remove and secure the device/s at the earliest possibility, if this is permitted by your school or education sectors policies.
- If you are involving the police the material may be required for evidence purposes – where possible, maintain observations of the device in the presence of a witness. Request the student does not touch the device until police arrive, to prevent the loss, concealment or destruction of evidence. This may have a crucial impact on whether any action can be taken in the circumstances.
- Obtain passwords/passcodes from the student if possible.
- If the student refuses to hand over the device, wait for parental consent or for police to arrive.
- If the intimate image or video is contained on a shared school device (such as a library computer), notify the school's ICT administrator to quarantine the device from the network.

Police involvement

Police response and involvement will vary, as each State and Territory has its own specific laws around children and young people under 18 sharing intimate images and videos without consent.

There are also criminal laws designed to protect children and young people under 18 from serious harm caused by the production, viewing and exchange of child sexual exploitation and abuse material.

When police respond to image-based abuse involving school student/s, they may need to speak with the student/s involved. Victims may find it easier to speak about intimate images and videos without their parents/carers or a teacher present. Police will generally leave the decision up to the young person to ensure they feel comfortable. This is in keeping with best practices in dealing with crimes of a sexual nature. However, in some cases police may speak only with the parents/carers and not with the student/s.

If a student is a potential suspect, the police will interview them in the presence of an adult.

After police have assessed the situation, they will determine the most appropriate action to take in consultation with the affected students and their family.

Possible pathways include:

- an educative or restorative approach involving talking with students and parents/carers, rather than placing the person responsible before the courts, and possibly suggesting resources and or services from helping agencies
- an investigative approach involving collecting further information and investigating with a view to potentially charging the person responsible.

Decisions to investigate and charge are at the discretion of police, who will consider the nature and seriousness of the conduct involved.

eSafety involvement

eSafety has legislative powers to help with the removal of intimate images and videos that have been shared without consent. We work with online service providers to have this done. We can also work with the police, if they are involved, and share information with them. In some cases, eSafety may take civil action against the person responsible for sharing the intimate image or video, but eSafety cannot take criminal action ourselves.

Image-based abuse can be reported to eSafety by:

- the person in the intimate image or video
- a person authorised on behalf of the person in the intimate image or video
- a parent or guardian on behalf of a child who is aged under 16 or who has a condition that makes them incapable of managing their own affairs.

Ongoing support and resources

Reputational damage to the organisation should not be the basis upon which support decisions are made. **Australia's Royal Commission into Institutional Responses to Child Sexual Abuse** has highlighted this. The wellbeing and protection of the students involved including the victim, alleged offender and witnesses should always be the primary concern.

Consider developing a communication plan so that everyone is provided with the same information at the same time. Media enquiries may come because of a lack of information which can lead to individuals filling in the void with inaccurate information themselves or seeking this detail publicly.

Consider whether the incident requires individualised follow-up contact with those involved in line with police advice, and/or whole-of-school communication about the resolution of the incident, again in line with police advice.

Further guidance on addressing critical incidents can be found in the **Toolkit for Schools – RESPOND element**.

There are several services that can be used to provide support and resources for students, parents and carers, and teachers and other school staff, including:

eSafety

eSafety.gov.au

eSafety can help with the removal of intimate images or videos that have been shared without consent. Reports can be made here: **Report online harm | eSafety Commissioner**. The eSafety website provides evidence-based and **curriculum-aligned classroom resources**, **teacher professional learning** and advice for **parents/carers** covering a range of online safety issues.

Australian Centre to Counter Child Exploitation

accce.gov.au

The Australian Federal Police (AFP) lead the Australian Centre to Counter Child Exploitation (ACCCE — pronounced 'ace'). It focuses on countering online child sexual exploitation (including sexual extortion) within organised child exploitation networks operating in online environments. eSafety works closely with the ACCCE.

Support services

Bravehearts Crisis Support and Counselling
bravehearts.org.au
Tel: 1800 272 831
A specialist support service for children and young people affected by sexual assault.

headspace
headspace.org.au
An early intervention mental health service for young people aged 12 to 25 years, including a 24-hour crisis support and suicide prevention service.

Kids Helpline
kidshelpline.com.au
Tel: 1800 55 1800
A free, confidential telephone and online counselling service for young people aged5 to 25 years.

ReachOut
au.reachout.com
An online youth mental health service. ReachOut provides information, support and resources about mental health issues.

Published 06/2025