Australian Government

TOGETHER AGAINST BULLYING

Responding to cyberbullying, image-based abuse and online harm among students

Who is this resource for?

All school staff.

Resource purpose

This guide supports school staff in responding to cyberbullying or other forms of online harm, including image-based abuse, when it is first observed or reported. It focuses on bullying behaviours, including harmful antecedent behaviours (referred to throughout this resource as bullying and other harmful behaviours). Antecedent harmful behaviours are behaviours that cause harm and, if left unaddressed, may continue or escalate over time. It outlines the immediate steps staff should take to support students, preserve relevant evidence, report concerns and escalate them where required. The guide also describes how the school's nominated person coordinates the ongoing response following the initial report, including assessment, investigation, support and reporting, in line with current eSafety Commissioner guidance.

The guide should be read in the context of relevant school and school system policies, procedures and frameworks.

Key practice question

What does the student need to feel safe and supported, and what information, reporting or escalation is required?

Quick reference guide

Key messages

1. **Put safety and wellbeing first.**
   Listen calmly, acknowledge the impact and respond without blame. Staff do not need to establish every detail before supporting the student.

2. **Preserve information safely.**
   What you should preserve depends on the content. Do not access, copy, save or share illegal, restricted or high-risk material. Follow school procedures and current eSafety guidance.

3. **Report and escalate promptly.**
   Record relevant information and follow school reporting pathways. Immediately escalate concerns involving high-risk material, including threats, coercion, possible adult involvement or a serious risk of harm.

4. **Consider everyone involved.**
   Consider students who experienced, caused, witnessed, shared or otherwise contributed to the harm, and identify who needs support.

Know your role: initial response to online harm

All school staff:

First response and report:

- check the student's safety and wellbeing
- listen and acknowledge their experience
- record relevant information where appropriate
- document actions and follow reporting and escalation procedures.

Report to the principal or nominated response person or team

Report concerns promptly to the principal or the school's nominated response person or team (in line with policy). Immediately escalate concerns involving image-based abuse, threats, extortion, coercion, possible adult involvement, illegal or restricted material, or an immediate or serious risk of harm.

Staff are not expected to investigate the incident, decide whether a law has been broken or manage complex online harm alone.

Principal or nominated response person:

Investigate and coordinate (in line with eSafety guidance)

- assess the student's safety, wellbeing and support needs
- identify reporting and referral requirements
- develop and coordinate a safety and support plan
- communicate with the student and their parents or carers, as appropriate
- coordinate follow-up and ongoing support.

Staff should comply with all safeguarding, child protection and mandatory reporting requirements applicable to their role.

Initial response to cyberbullying and online harm

Quick decision guide for all school staff

This flowchart acts as guidance only and should be applied in the context of your school and education sector policies, safeguarding procedures and reporting pathways.

A concern is observed, disclosed or reported

1 Check immediate safety

Is anyone in immediate danger? Is urgent health, wellbeing or emergency support needed? Stay with the student where required and obtain assistance in line with school procedures.

Unsafe: Act now

Contact the principal or school leader immediately. Use emergency and safeguarding pathways required by policy.

Consider escalation pathways, for example:

- mandatory reporting guide and child protection
- police and/or ACCCE*
- eSafety Commissioner
- school ICT/cyber security team
- emergency services (000) where there is an immediate threat to life, health or safety.

Safe

2 Listen, support and explain next steps

1. Listen without judgement.
2. Acknowledge the impact.
3. Reassure the student that reporting was the right step.
4. Do not promise confidentiality.
5. Explain that the concern must be shared with the school's nominated response person.

Continue next page

*ACCCE is the Australian Centre to Counter Child Exploitation

Does the concern involve other harmful online content, or suspected illegal, restricted or high-risk material?*

Other harmful online content*

a

Record available information

Where appropriate, support the student to retain non-restricted details such as screenshots, URLs, usernames, dates and times in a secure location. Do not ask the student to view or repeatedly collect harmful content. Not all information can be preserved. If unavailable, continue to support the student, record what is known and follow the same reporting and escalation process.

Illegal / restricted / high-risk**

b

Do not access or reproduce the material

Do not open, view, copy, screenshot, save, store, forward or share suspected illegal or restricted material. Record only contextual details, such as the account, URL or location, without reproducing the material. Escalate immediately. If you are unsure which pathway applies, do not access or reproduce the content. Refer the concern immediately to the nominated response person.

3

Take practical steps to limit further harm

Ask students not to share, forward, repost, comment on, react to or tag others in the content. Encourage reporting. Support the affected student to block or restrict relevant accounts and review privacy settings where appropriate. If staff or the student do not know how to do this, enlist support from appropriately skilled school personnel. Do not access the student's account yourself.

4

Record the concern

Use approved school systems. Record factual information, the student's immediate needs, actions taken and who has been notified. Protect privacy and share information only with those who need it.

5

Report every concern

Report and escalate every incident promptly to the school's nominated response person, principal or designated school leader identified by school policy. High-risk concerns are escalated immediately. Initial staff do not investigate or decide whether an offence has occurred.

Refer to school's nominated response person (in line with school policy)

Ongoing assessment and response

(Guided by eSafety and in line with school and education sector procedures)

The nominated response person assesses the incident's severity, risk and impact and coordinates the ongoing response. This includes determining appropriate safeguarding, family communication, reporting, referral and support pathways, coordinating support for the student, and managing relevant information and follow-up.

Escalation pathways

If a report needs to be escalated, the nominated person draws on guidance from eSafety and the Response Pathways Resource to determine the appropriate next steps. The nominated person consults with relevant staff to decide how the report should be escalated and brings in whoever is needed to ensure the report is managed safely, thoroughly and in line with school and education authority procedures.

*Other harmful online content: Messages, images, videos or other online material that may distress, intimidate, threaten, humiliate or otherwise harm a student.

**Illegal or restricted online content: Seriously harmful material or material unsuitable for children and young people, including child sexual abuse material, pro-terror content, detailed nudity or high-impact violence. Adapted from: eSafety Commissioner. (2025, October 7). What is illegal and restricted online content? Australian Government. www.esafety.gov.au/report/what-is-illegal-restricted-content

Understanding the context

When online harm happens outside school

Schools are not responsible for all online behaviour. Some online incidents may occur outside the school setting, either among students from the same school or between a student and someone they know through sport or another community activity.

However, when online behaviour affects a student's wellbeing, learning or participation at school, staff may need to support the student and address those impacts, regardless of where the behaviour occurred or who was involved.

This may include working in partnership with families, parents or carers to understand the impact on the student and coordinate support.

What should staff do?

Follow school policies and procedures to consider:

- how the student and school environment are affected
- what support the student needs.

Consider students' roles and the wider context

Students involved in online harm may not fit neatly into categories based on whether they have experienced or caused harm. Some students may:

- move between roles in different situations, such as causing harm online while experiencing harm offline
- witness, encourage, share or spread harmful behaviour or content

Understanding students' roles, peer dynamics and relationships can help staff avoid assumptions, identify support needs and respond to the wider context.

Questions to consider

- who experienced, caused, witnessed, encouraged or shared the harm?
- is it part of an ongoing conflict or pattern?
- does it involve identity-based harm, for example harm targeting the student's culture, religion, disability, sexuality or gender?
- is the harm occurring online and offline?
- who else may need support?

What is different about responding to online harm

Consideration	Practice point
Content can spread quickly	Ask students not to share, repost, comment on, react to or tag others in harmful content. Support students to use blocking and reporting tools.
Relevant information may need to be preserved	The appropriate steps depend on the nature of the content. Follow school procedures and relevant guidance (see quick decision guide).
Additional reporting pathways may apply	This may include reporting to the platform or eSafety.
More students may be involved or affected	Consider everyone who engaged with the content, including students affected by witnessing identity-based harm.
Students may need online safety support	This may include blocking, muting, privacy and account security features. Refer to the eSafety Guide on the eSafety website for platform-specific support.
The full picture may be unclear	Gather relevant information recognising that content may be deleted, hidden, anonymous or dependent on context. You do not need to establish every detail before supporting and reporting the concern.



AI-generated or manipulated content

AI can be used to create or alter text, images, audio or video to impersonate or harm someone.

AI-generated or manipulated content can cause significant harm even when people know it is fake.

When responding:

- do not ask the student to prove that the content is false or AI-generated
- consider whether it may be image-based abuse and follow current eSafety guidance
- monitor ongoing sharing, impersonation, harassment or reputational harm to the student
- follow school reporting pathways, even if the original content has been removed.

Detailed guidance for responding to online harm

The response flowchart provides an overview of the process. The following sections provide more detailed guidance on preserving information, reporting and escalation, and student support.

How to preserve evidence

First, identify the type of content

1 Suspected illegal, restricted or high-risk material

Content that is seriously harmful or unsuitable for children and teenagers, such as child sexual abuse material, pro-terror content, detailed nudity or high-impact violence.

DO NOT open, view, copy, screenshot or record, save, store, forward or share the intimate material.



If you have accidentally sighted the material, close immediately.

Possessing or sharing intimate images, such as nude, partially nude or sexual images, of a person under 18 may constitute a child abuse material offence under Commonwealth or state and territory law, including where the images are real, digitally altered or AI generated.

- ✔ consult eSafety guidance on preserving evidence and reporting the content
- ✔ **with the student's consent, record only contextual information, such as when and where it was shared (e.g., the app, platform or game name), the account name, username, URL, location, dates and times, without reproducing the material (for more details see eSafety's: *how to collect evidence resource*)**
- ✔ refer the concern immediately to the school's principal or nominated response person, in line with school policy.

2 Other harmful online content



This includes online messages, comments, images, videos or other material that may upset, distress, intimidate, threaten, humiliate or otherwise harm a student but is not necessarily illegal or restricted.

- ✔ consult the eSafety website (www.eSafety.gov.au). Where appropriate, support the student to record and retain available information such as screenshots, URLs, usernames, dates and times. See www.esafety.gov.au/report for further information
- ✔ if information cannot be preserved, record what is known and continue with the reporting and escalation process. Reassure the student that the issue will still be addressed
- ✔ do not ask the student to view or repeatedly collect harmful content or to provide evidence if this may cause further distress
- ✔ in line with school policy, report all incidents to the school's nominated representative.

For both explicit and non-explicit harmful content



- ✔ ask the student targeted and any other involved students not to share, forward, repost, comment on, react to or tag others in the content
- ✔ support the student to block or restrict relevant accounts and review privacy settings, where appropriate (if the student doesn't know how to do it, see eSafety guide or nominate a skilled person from school)
- ✔ follow all safeguarding, child protection and mandatory reporting requirements that apply to your role.

Case study: responding to cyberbullying

This case study shows how school staff can respond when a student discloses cyberbullying.

A Year 11 student tells her teacher that classmates created a messaging group where they post hurtful comments about her and share them with others. They add her to see the messages and then remove her. She arrives at class distressed and worried.

Initial response: What the teacher or first responder does:

1 STEP 1: Safety first

The immediate response depends on the situation. If a student is distressed, staff may need to:

- ✔ arrange class supervision or seek help from another staff member
- ✔ move to a space where the student can talk without being overheard, while remaining visible to other staff
- ✔ ensure the student is not left alone if there are safety or wellbeing concerns.

2 STEP 2: Support the student

- ✔ listen calmly and take the report seriously
- ✔ reassure the student that they did the right thing by seeking help
- ✔ explain what will happen next and involve them in decisions about their support
- ✔ explain that the concern must be reported and do not promise confidentiality.

3 STEP 3: Report and record

- ✔ without reproducing the material and with the student's consent, ask the student to preserve available evidence, including screenshots, the platform, account name or username, URL, relevant dates and times, and when and where the material was posted, until they meet with the school's nominated person
- ✔ suggest that they avoid repeatedly viewing or engaging with the material
- ✔ report the concern promptly to the school's nominated person
- ✔ document what the student has shared, including any available evidence described above, actions taken and the person notified.

4 STEP 4: Prevent further sharing

- ✔ advise the student not to share or distribute the material
- ✔ check whether other students are continuing to share, like or comment on it, and direct them to stop.

5 STEP 5: Stay within your role

- ✘ do not investigate the incident
- ✘ do not attempt to determine whether an offence has occurred.

Ongoing response: who does what?

Some students may need extra support to report, understand or respond to online harm. Avoid making assumptions about what a student needs.

Consider how disability, language and communication needs, experiences of trauma and discrimination, wellbeing, cultural background, religion, gender, sexuality, family circumstances or other factors may affect the student's experience and support needs.

Use trauma-informed principles throughout the response. Build on the student's strengths and tailor support to their individual needs and preferences, including through accessible and culturally safe support.

Role	Key responsibilities	Trauma-informed focus
Executive staff / nominated response lead	› coordinate the ongoing response › follow school procedures and current eSafety guidance › check in on staff who handled initial report.	**Be clear and predictable** › keep the student informed and avoid placing responsibility for resolving the issue on them.
Wellbeing staff	› support coping and ongoing wellbeing needs › involve the student in planning for attendance, classes and peer interactions › provide communication adjustments or alternative ways to communicate.	**Support voice and choice** › ask what support feels safe and useful to the student.
Administration / IT	› protect privacy and maintain confidentiality (where appropriate) › store and coordinate records appropriately › support necessary communication › assist with blocking content where appropriate.	**Protect dignity and privacy** › handle information and harmful content sensitively.

Staff wellbeing matters too

Responding to serious online harm can be challenging. Staff should consider seeking supervision, debriefing or wellbeing support in line with school procedures (see eSafety's educator toolkit at www.esafety.gov.au/educators/toolkit-schools/respond for more information).

Further information

For detailed guidance on reporting, evidence collection, platform-specific reporting tools, cyberbullying, image-based abuse and emerging online harms, refer to the eSafety Commissioner website at: www.esafety.gov.au.

Specifically, for responding to and reporting instances of online harm, please refer to www.esafety.gov.au/educators/toolkit-schools/respond and www.esafety.gov.au/report.

Spotlight on Cyberbullying is also available at www.esafety.gov.au/educators/spotlight-on-cyberbullying.

Where to get more help

Beyond Blue: 1300 22 4636 or beyondblue.org.au. Mental health support for stress, anxiety and overwhelm.

Lifeline: 13 11 14 or lifeline.org.au. Crisis support and counselling if things feel overwhelming.

13YARN: 13 92 76. Culturally safe support for Aboriginal and Torres Strait Islander peoples.

1800RESPECT: 1800 737 732 or 1800respect.org.au. Free support for people impacted by domestic, family and sexual violence.

eSafety Commissioner: eSafety.gov.au. Report cyberbullying, get advice, and request content removal support.

Australian Human Rights Commission: humanrights.gov.au. Support for cases involving discriminatory harm. Reports can be made via the website or by emailing infoservice@humanrights.gov.au.

Medicare Mental Health: Visit medicarementalhealth.gov.au or call 1800 595 212 to find free mental health services and Medicare Mental Health Centres.

QLife: 1800 184 527 or qlife.org.au. Peer support and referral for LGBTQIA+ people.

Kids Helpline: 1800 55 1800 or kidshelpline.com.au. Free counselling and support for children and young people aged 5–25 years.