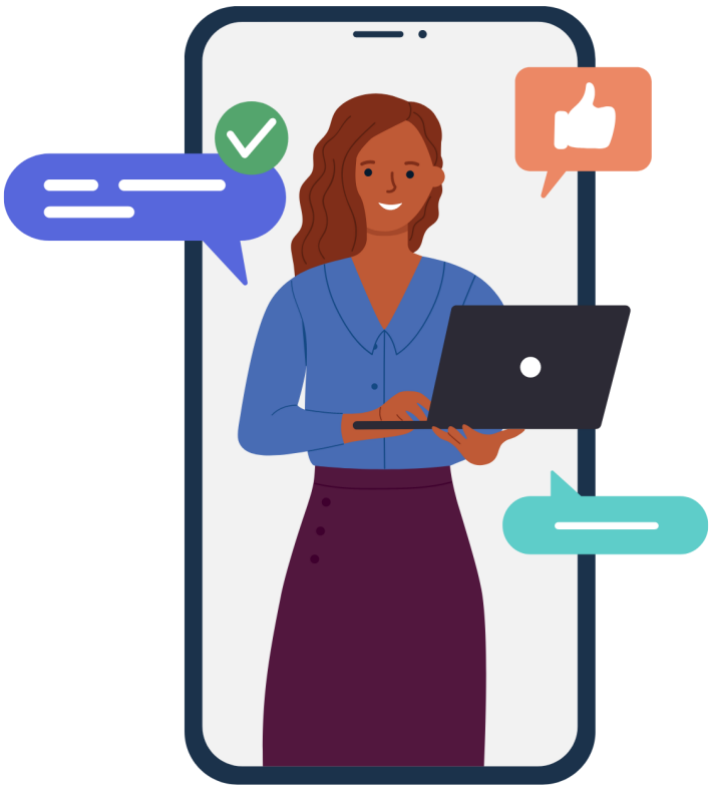
Guide to responding to online abuse that targets staff

Creating safer online environments



Why has this guide been produced?

This guide provides advice for Australian schools about how to respond when school staff are the targets of online abuse. It should be read alongside school and/or education sector policies and procedures.

What is adult cyber abuse?

Important note

Bullying, aggression and abuse directed towards school staff is a serious issue. Being targeted by other members of the school community can have a serious and negative impact on mental health and wellbeing, and their ability to perform in their role.

The Australian Government Department of Education's Anti-Bullying Rapid Review highlighted that the right to a safe workplace is a fundamental principle enshrined in Australia's work health and safety laws. All school staff should feel empowered and confident to speak up if they experience or witness any form of bullying or abuse, online or offline.

Principals and school leaders play a key role in building a positive learning and working environment where the whole school community feels included, connected, safe and respected.

Adult cyber abuse is defined in the Online Safety Act 2021 (*Cth*) as material, communicated through a social media service, relevant electronic service or designated internet service targeting an Australian adult (aged 18 years or older) that is both: intended to cause serious harm, and menacing, harassing or offensive in all the circumstances.

If the material meets only one of the two criteria above (for example, if the post is offensive but is found to not be intended to cause serious harm), it will not be considered adult cyber abuse under the Act.

Under the Act, the term 'adult cyber abuse' is reserved for the most severely abusive material intended to cause serious psychological or physical harm. This would include material which sets out realistic threats, places people in real danger, is excessively malicious or is unrelenting.

eSafety has published the following resources to assist:

- Adult cyber abuse information
- Online abuse in the workplace – employer information
- Online abuse in the workplace – worker information

Online abuse of school staff can take place using online chat and video messaging services, on social media, in online classrooms or learning management systems, in text messages, in emails, on message boards and in online forums that allow people to comment publicly or provide ratings.

These are some examples:

- Making targeted and persistent personal attacks online that ridicule, insult or humiliate a person, or make others think badly of them. If the attacks relate to their physical appearance, religion, gender, race, disability, sexual orientation and/or political beliefs this is sometimes known as online hate.
- Sharing, or threatening to share, an intimate image or video of someone without their consent. This is known as image-based abuse. It includes 'deepfake' AI generated images and videos.
- Blackmailing someone by threatening to share a nude or sexual image or video of them unless they give into demands for money or something else. This is a form of image-based abuse, known as sexual extortion.
- Cyberstalking, which is when someone keeps constant track of a person online in a way that makes them feel uncomfortable, worried or threatened.
- Posting someone's personally identifiable information online without their consent, to make them feel unsafe, which is known as doxing. An example is sharing their phone number or home address on social media and saying they are available for sex, so strangers call or visit them.
- Threatening violence or inciting others to do the same – such as saying a person should be killed or raped, whether it leads to assault or not. Encouraging someone online to self-harm or suicide.

Depending on the nature of the material posted or transmitted, some types of online abuse may also be criminal offences.

1. Managing incidents

If there is a staff member is in immediate danger or at risk of harm, call emergency services on Triple Zero (000).

If there are threats to a staff member's personal safety or threats to their family or friends, contact police on 131 444.

If any staff member discloses that they are being targeted online, the school leadership team should work with them to resolve the issue in a timely manner. Online abuse is never acceptable and should never be dismissed as a routine part of staff work.

Report to the principal or nominee any online abuse that may be considered a risk to safety or wellbeing or that may compromise the good order and management of the school.

- If a parent/carer is targeting a staff member online, the staff member should never respond or retaliate. A member of the school leadership team may invite the parent/carer to a meeting to address their concerns and, if they have a reasonable complaint, they can

be reminded of the appropriate ways to raise issues with the school and can be requested to remove offending content. If they refuse, the school leadership team should follow school and/or education sector policies and procedures.

- If a student is targeting a staff member online, the school should take steps to minimise harm in accordance with their duty of care to both staff and students. This can involve supporting the staff member to have the content taken down as quickly as possible and supporting the student to understand online behaviour expectations.
- If a colleague is targeting a staff member online, it should be dealt with through the relevant code of conduct and human resources processes.
- If a fellow staff member is being targeted, a fellow student is being targeted, be an 'upstander' instead of a bystander by encouraging them to report it to an appropriate staff member and sharing eSafety's advice with them.
- If the incident relates to domestic, family and sexual violence you may wish to contact **1800RESPECT** (1800 737 732). Remember, your safety is important. If an abusive person learns that you are seeking resources and information, their behaviour may get worse. To help manage the abuse, learn more and connect with support.

It's important to find out the relevant information, collect any evidence and keep accurate written records of the incident and outcomes, being mindful of the staff member's privacy.

The process to resolve online incidents should aim to restore relationships in a way that promotes the safety, wellbeing, privacy and procedural fairness for everyone involved.

If repeated incidents occur, disciplinary procedures should be followed.

2. Collecting evidence and reporting

If working with members of the school community does not resolve the problem, there are alternative pathways for help and support.

School leaders should first obtain the staff member's consent if acting on their behalf.

Staff members can take the following steps to report serious online abuse and have harmful content removed:

1. Collect evidence – take screenshots of what has happened and which service or platform it occurred on. Take note of the usernames of the accounts that have been used to target you, the webpage address or URL where the harmful content appeared, the dates and times the content was sent or shared. Instructions for how to collect evidence can be found here: How to collect evidence | eSafety Commissioner.

2. Report it – to the service or platform, and then to eSafety.

- Harmful posts, comments, messages and profiles should first be reported to the online platform or service. If they don't help, and the abuse is very serious, report it to eSafety.
- Sharing or threatening to share an intimate image or video of you without your consent is image-based abuse – it can be reported to eSafety immediately unless

you're being blackmailed. If you're being blackmailed, go to our advice on how to deal with sexual extortion.

3. Stop contact – tighten your security settings and prevent content from being shared further.

3. Legal action

Serious adult cyber abuse can be a crime. The police may be able to help.

Some other forms of online abuse are illegal under state, territory or federal legislation. Information about getting legal help is available on the eSafety website. Legal advice can help the targeted staff member determine how to address the online abuse. Education unions, professional associations, community legal centres or Legal Aid may be able to provide advice.

Read information about the difference between serious online abuse and defamation.

4. Ongoing support

School leaders can help staff by promoting the services of employee assistance providers, union representatives, wellbeing representatives and external agencies if required.

Encourage staff to check eSafety's website for a list of counselling and support services, which can be filtered by audience, the type of support required and state/territory.

School leaders should consider whether an incident requires follow-up communication with those involved or to the whole school to help address the issue.

See eSafety's tips for managing the impacts of adult cyber abuse, image-based abuse or child cyberbullying.

Learn more about what can be reported and use eSafety's summary table, which outlines different forms of online abuse and ways to deal with it. If the online experience does not fit the criteria for eSafety to investigate, it may be helpful to learn about the other options available.