



Guide for dealing with online abuse of tertiary staff



This guide provides advice about how to deal with online abuse that targets staff. It complements the [Principles for dealing with online incidents](#) resource and should be read alongside your relevant institutional policies.

Experiencing online abuse can have serious negative impacts on a person's mental health, wellbeing and ability to perform in their role. Both staff and students need to feel empowered and confident speaking up if they experience, or witness, any form of abuse, either online or offline.



What is online abuse?

Online abuse can take place on social media, through online chat and video messaging services, in online classrooms, in text messages, in emails, on message boards and in online forums that allow people to comment publicly. 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 or sexual photo 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](#).
- Encouraging someone online to self-harm or suicide.
- [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.



Managing incidents

Do you feel unsafe right now?

If you are in Australia and in immediate danger or at risk of harm, call emergency services on Triple Zero (000).

If there are threats to your safety or threats to your friends or family members, contact your local police on 131 444.

If any staff member discloses that they are experiencing online abuse, relevant senior staff should collaborate with them to help resolve the issue in a timely manner.

- If a colleague is targeting a staff member online, it should be dealt with through the relevant human resource team.
- If a student is targeting a staff member online, steps will need to be taken by the institution to minimise harm in line with their duty of care to both staff and students. This can involve supporting the staff member to have the abusive content taken down as quickly as possible and supporting the student to understand online behaviour expectations.
- 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 any online incident 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.



External reporting

In addition to referring to your institution's policies and procedures, you can suggest the staff member takes the following steps to report serious online abuse and have harmful content removed:

- 1. Collect evidence** – [take screenshots](#) of what has happened and which platform it occurred on.
- 2. Report it** –
 - Harmful posts, comments, messages and profiles should be reported to the online platform or service first. 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.
- 4. Get more support** – check 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 how using 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](#).

Note: Remember to obtain consent if you are taking any action on behalf of anyone else who may be experiencing online abuse.



Ongoing support

You can help the staff member by providing referrals to employee assistance providers, human resources and external [counselling and support services](#), if required.

Senior staff should consider whether an incident requires follow-up communication with the person targeted or other staff or students, or further action to help manage the issue.

In addition, eSafety offers:

- a range of [free professional learning and resources for staff](#), providing an overview of eSafety's key functions, the risks faced by people of varying ages and backgrounds, and the latest research and trends in online safety
- free workshops for [frontline workers](#) who support staff and students through online abuse relating to domestic and family violence.

