Guide for students
responding to cyber abuse

Toolkit for Universities
Creating safer online environments

This guide provides university students with advice about how to respond if they are the target of cyber abuse. Cyber abuse is behaviour that uses technology to threaten, intimidate, harass or humiliate someone — with the intent to hurt them socially, psychologically or even physically.

Experiencing cyber abuse from within your university community can have a serious and negative impact on your mental health, wellbeing and ability to access or complete your studies. All university students should feel empowered and confident speaking up if they experience or witness any form of bullying or abuse — online or offline.

Types of cyber abuse

Cyber abuse can take place on social media, through online chat and messaging services, in online classrooms, in text messages, in emails, on message boards and in online forums that allow people to comment publicly. It includes:

- Stalking a person online and hacking into their accounts e.g. social media, banking or email accounts. This is known as 'cyberstalking'.
- Sharing intimate or sexual photos or videos online without consent — also known as image-based abuse.
- Targeted and persistent personal attacks aimed at ridiculing, insulting, damaging or humiliating a person — this might relate to someone's physical appearance, religion, gender, race, disability, sexual orientation and/or political beliefs. This is known as online hate.
- Encouraging someone to self-harm and/or suicide.
- Posting someone's personal information on social media or elsewhere online along with offensive and/or sexual comments — resulting in calls and visits from strangers.
- Threatening violence or inciting others to do the same — such as threats of death and sexual assault that might lead to physical contact and/or assault.

Managing incidents

When an online incident involves university staff or other students, refer to your university's relevant policies or code of conduct alongside the advice in this guide.

If you believe you are a target of cyber abuse and are feeling unsafe right now, call the police on Triple Zero (000) or 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.

You can also learn more in eSafety's cyber abuse response guide — a valuable resource that outlines different forms of cyber abuse and ways to respond. Share this resource with any friends or classmates impacted by cyber abuse.

General guidelines:

- If another student is targeting you online, consider raising this with your tutor or lecturer, the course coordinator and/or your university's student safety or welfare officers.
- If a university staff member is targeting you online, approach another staff member in your school or faculty to escalate the matter. Other avenues you can explore include student services, the university's equal employment office or anti-discrimination unit, the equity office, or the human resources unit of the university.
- For any incident where a student you know is targeted — speak to the student and offer support if it is safe and appropriate to do so. Provide the student with links to eSafety's cyber abuse response guide, listen to them and advise them that student welfare staff/professional services staff in your school or faculty may be able to help to improve, or resolve, the situation. You may want to offer yourself as support in meetings with university staff.

Content removal

In addition to speaking with your university there are other support pathways for those experiencing cyber abuse. These include:

- Reporting the abuse to the relevant social media service. Depending on the service, it may be an option to block, report or mute the abuse. The eSafety Guide has links to the latest platforms, apps and social media and tips on how to report abuse.
- Reporting image-based abuse to eSafety.
- Seeking support — you don't need to deal with cyber abuse alone.

If you plan to make a report, you may need to collect evidence, including screenshots/prints of messages or web pages. The eSafety website provides detailed information about how to do this.

Remember to obtain consent if you are taking action to help someone experiencing cyber abuse.

Legal action

Some forms of cyber abuse are illegal under state or federal legislation and legal advice can help you determine how best to address the abuse. Visit eSafety for a list of legal and support services.

Ongoing support

If you, or another student, need ongoing support you can visit your university's student counselling service. Information about services will be available on your institution's website. There are also a number of external support services that can offer support during this time.

Published 05/2020