Guide for universities responding to cyber abuse against staff

Toolkit for Universities

Creating safer online environments

This guide provides universities with advice about how to respond to cyber abuse that targets staff. It should be read alongside relevant institutional policies.

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.

Australian Government

eSafety Commissioner

UNIVERSITIES AUSTRALIA

esafety.gov.au

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 the university community can have a serious and negative impact on a staff member's mental health, wellbeing and ability to conduct their role. Staff, as well as students, need to feel empowered and confident to speak up if they experience, or witness, any form of bullying or abuse, either online or offline. University leaders should play an active part in building a positive learning and working environment — where the whole university community feels included, connected, safe and respected.

Examples of cyber abuse:

- 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 — this is also known as image-based 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 can include:
  - 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 ('online hate' targeting an individual).
  - 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.

Managing incidents

If any staff member discloses that they are experiencing cyber abuse, relevant senior staff should collaborate with them to help resolve the issue in a timely manner. Adults experiencing cyber abuse can visit eSafety for general advice and guidance, including information about when to seek legal advice and where to go for legal assistance. eSafety's cyber abuse response guide may help staff in identifying appropriate actions, including reporting the abuse.

A variety of support services, including 1800RESPECT (1800 737 732), can also help.

Managing a response

- If a colleague is targeting a staff member online, it should be dealt with through the university's human resources unit.
- If a student is targeting a staff member online, the university will need to take steps 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.
- If it is safe and appropriate to do so, a face-to-face conversation with the staff member and other parties involved may assist in achieving a resolution. The staff member concerned may wish to have a support person involved in any meetings.
- 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 occurred, university disciplinary procedures should be followed.

Content removal

eSafety and support agencies can help to address cyber abuse alongside actions being taken by the university. Remember that, when taking any action on behalf of the staff member, they must have provided consent.

Consider advising any staff member who has experienced cyber abuse to:

- Report the abuse to the social media service. Depending on the platform, it may be able to block, report or mute the abuse. The eSafety Guide has links to the latest platforms, apps and social media with tips on how to report abuse to them.
- Report any image-based abuse to eSafety.
- Seek support from counselling or other services — remind them that they do not need to deal with cyber abuse alone.

To make a report, the staff member targeted may need to collect evidence, taking screenshots/prints of messages or web pages, including the URL where relevant, and recording the date and time.

Legal action

Some forms of cyber abuse are illegal under state or federal legislation. Legal advice can help the targeted staff member determine how to address the abuse and can also help an accused member of the university community to respond if legal action is taken against them. Visit eSafety for a list of legal and support services. Universities may also wish to consult with their legal counsel on appropriate courses of action.

Ongoing support

Universities can help staff by providing referrals to employee assistance providers, human resource units and external agencies, if required.

A university's senior staff should consider whether an incident requires follow-up communication with those involved, or to the whole university, to help manage the issue. Support services can help with the ongoing education of staff and students.

In addition, eSafety can deliver free webinars to university staff that provide an overview of eSafety's key functions, the issues facing adults, the latest research and trends in online safety.

eSafety Women also offers free two-hour workshops for university frontline workers who support staff (and students) through cyber abuse relating to domestic and family violence.

Published 05/2020