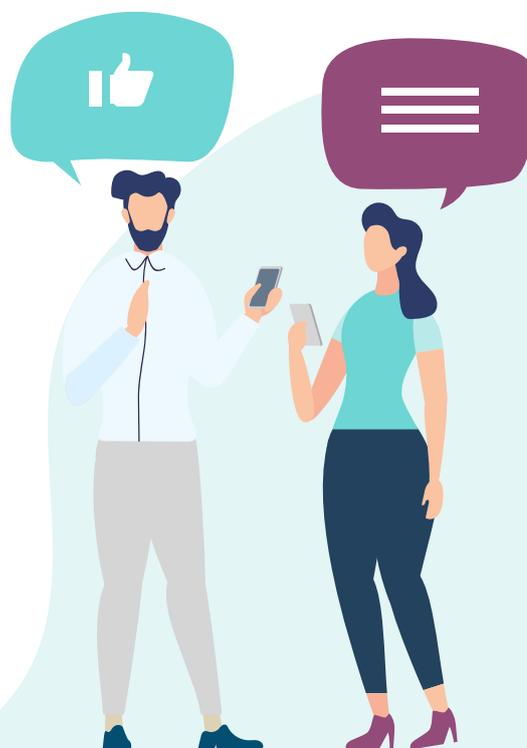


# Creating a safer online environment

## Toolkit for Universities

Creating safer online environments



This resource provides general guidance about how to establish and maintain a safe online environment for the university community. It can help to frame an institution's approach or assist in identifying actions to create a safer online environment.

**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.



Universities can work toward safer online environments by reviewing, assessing and adopting the following as appropriate.

## Environment and policies

Universities can:

- Encourage a culture of help-seeking that supports students and staff to feel safe and comfortable in reporting online incidents.
- Have a strong 'no bullying' attitude and encourage respectful behaviour.
- Include physical and online safety in the institution's mission and values.
- Consider developing policies and procedures that address online safety. This will help to safeguard against, and respond to, online safety incidents.
- Specify online safety in relevant policies and procedures, teaching/learning materials and environments, communications materials and through social media.
- Set out expectations and make clear the behaviour that is/is not acceptable for students/staff when engaging with the university community online or using digital technologies for university-related purposes.
- Take a victim-centred approach in responding to online safety incidents and supporting those affected.
- Consider establishing an online safety team that has responsibility for, and champions, online safety. This team might include senior leadership, human resources staff, student services staff, technologies staff, academic staff, as well as students and student leaders.
- Communicate to the university community, what is considered acceptable use of the university's name, logo and brand. This includes clubs and societies, or other groups, that may use the institution's name, logo and brand on social media pages or accounts.

## Community safety and wellbeing

To support the online safety and wellbeing of the university community, it is important for institutions to:

- Involve the whole university community in online safety, this includes opportunities for meaningful student participation and engagement.
- Support staff and educate students about positive and safe online experiences. This is an important part of a comprehensive approach to online safety.
- Have clear procedures in place so that if an online safety incident is reported, students and staff know what to do and where to access help.
- Consider using preventative, harm minimisation and incident management strategies to support everyone involved in online incidents.
- Strengthen the effectiveness of incident responses and procedures to restore relationships by having partnerships with local police, external counselling and support services.
- Consider circumstances that could place students/staff at risk of harm if their image or information is shared prior to publishing content online, for example, where there are legal proceedings or a court order relating to sexual assault or family violence.



## Technology

To safely manage technologies, universities can:

- Endeavour to use software, online products and collaboration tools with the [highest safety, privacy and security standards](#).
- Conduct risk assessments to promote safety, privacy and security prior to using any platform or technology. The Toolkit resource: Risk assessment for new technologies and online platforms can help in assessing risks and benefits.
- Consider filtering to help monitor and limit what students access online, noting though that no filter is completely effective and should not replace online safety education for the university community.
- Establish responses to students/staff repeatedly trying to access/share harmful content that focus on safety and wellbeing.
- Be aware of the safety and security risks in using simple email naming conventions (e.g. students' real names) which can make it easier to identify and contact students. It is also important to use appropriate technologies to monitor and filter email activities on university ICT systems.
- Communicate the risk of inappropriate contact using university email addresses. Inform students/staff how to report unauthorised communication and block unknown email addresses to help minimise risk.
- Explain that it is unacceptable for students/staff to use university-affiliated platforms, email accounts or social media for image-based abuse, cyberbullying, harassment or other types of inappropriate behaviour. Consider addressing these behaviours in your institution's relevant health, wellbeing or safety policy (if not currently included).