



Cyber Safety Policy

Cybersafety and Responsible Use of Digital Technologies Policy

POLICY

This policy outlines measures AllU will take to support students to engage with digital technology in a safe and responsible way.

SUMMARY

AllU staff, volunteers, host families and third-party providers have a duty of care to students to take reasonable steps to ensure digital learning is conducted in a safe and responsible manner.

AllU will ensure students are aware of expectations relating to the safe, responsible and ethical use of digital technologies. Online incidents of concern will be managed in accordance with AllU's **Response to Critical Incidents Policy and Procedures** and **Child Safety Incident Report Form**.

When children/young people have access to internet-enabled devices, they also have access to an extensive amount of content across the internet, social media and other applications. All those involved in implementing AllU's programs have a responsibility to enable students to maintain healthy, life-affirming relationships online and to use technology safely.

AllU has zero tolerance across all of its programs and activities of any form of cyber bullying and the deliberate and repeated misuse of technology to harass, threaten, insult or ridicule students or staff. Examples include threatening texts, emails or direct messages, online denigration, vilification or defamation, derogatory websites, disturbing private pictures or videos, and online exclusion or impersonation.

It is important to note that victims of cyber bullying can include both students and adults.

AIMS

This Cyber Safety and Responsible Use of Digital Technologies Policy aims to maximise the benefits of the Internet and Information, Communication and Learning Technologies, while at the same time minimising the dangers and managing the risks of cyber bullying within all AllU's programs and activities.

Furthermore, it seeks to:

1. Develop and maintain effective cyber safety practices which maximise the beneficial use of information communication and learning technology (digital) for students.
2. Educate students, staff, volunteers, host families and third-party providers on how to use digital platforms safely and responsibly.
3. Enable students to learn how to protect their own privacy and not infringe the rights of others in an online environment.
4. Establish practices to on how to respond to inappropriate use of digital platforms that infringes the rights of others.
5. Ensure cyber safety involves the active promotion of cyber safe behaviours based on the safe, respectful and responsible use of internet and mobile phone technologies, and the taking of specific measures to remove the risks of any inappropriate and harmful use of these technologies.

MANAGING RISK

To manage risk and support the safe and responsible use of digital technologies, the following areas need to be considered.

Supervision when using digital technology in the classroom

Consistent with their duty of care to children and young people, all adults involved in AllU's programs are required to adequately supervise students when using digital technology.

Measures to ensure that ensure children and young people are appropriately supervised when engaged in online learning might include:

- regularly monitoring screens
- installing security passwords on devices
- actively reinforcing learning and behavioural expectations during all activities.

Cyber Safety Use Agreement

AllU ensures students are aware of behavioural expectations when engaging in digital activities, and requests that students sign a Cyber Safety Use Agreement before commencing all student exchange program activities. Whilst not a legal documents per se, this Agreement plays an important part in describing AllU's expectations on students themselves to be safe, responsible and ethical users of digital technologies.

AllU will also recommend to host families that they, if comfortable in doing so, discuss, develop and implement a similar 'host family agreement' at home. This will assist students to understand what is and isn't appropriate behaviour and that appropriate behaviour is expected everywhere and anytime they are online.

Student and AllU staff, volunteers, host families and third-party provider responsibilities

The ever-changing nature of the internet poses some unique challenges and opportunities for all of those engaged in AllU's programs and activities.

If any of the behaviours below occur when participating in any of AllU's programs, it will constitute a breach of the Cyber Safety and Responsible Use of Digital Technologies Policy, and AllU will be obliged to act accordance with its **Response to Critical Incidents Policy and Procedures** and **Child Safety Incident Report Form**.

Students and adults alike must be aware that in certain circumstances where a crime has been committed, they may also be subjected to a criminal investigation by the police over which AllU will have no control.

1. AllU's name or logo must not be used in any way which would result in a negative impact for the organisation, or anybody involved in its programs and activities.
2. Any materials created as part of AllU's program must not be posted online or distributed using any other technologies i.e. mobile phones, without permission from AllU.
3. Photos or videos of either themselves and/or other students or adults which denigrate, insult, humiliate or hurt those involved, or without their permission must not be posted online or distributed using any other technologies i.e. mobile phones.
4. All online communications are in keeping with the AllU's expectations in relation to appropriate and respectful interactions.
5. Inappropriate comments about individual students or adults, which if said in person, would result in disciplinary action being taken must not be posted online or distributed using any other technologies i.e. mobile phones.

6. Neither AllU's network nor a school's network nor the broader internet (whether accessed in situ or out, either during or after program hours, via any application) may be used for any purpose other than that which it was designed.
7. Cyber bullying, harassment, taking, sending and receiving naked or sexually explicit images (sexting), and other misuses of technology in cyberspace are unacceptable.

Students and adults involved in AllU's programs and activities who feel that they have been the victims of such misuses of technology should save and store the offending material on their computer, mobile phone or other device. They should then print a copy of the material and immediately report the incident to AllU using AllU's **Child Safety Incident Report Form**. Immediate contact with AllU is encouraged, even before the submission of the relevant Accident and Critical Incidents Report Form.

However, if the bullying material involves sexualised images, be aware that possessing or sharing such images of people under 18 may be a crime, even if you have just taken a screenshot for evidence purposes.

All reports of cyber bullying and other technology misuses will be investigated fully and may result in a notification to Police where AllU is legally obliged to do so. Sanctions imposed by AllU beyond any possible charges imposed by the Police, may include, but are not limited to, the loss of computer privileges or expulsion from AllU's program.

Host Families Responsibilities

Cyber bullying is a serious issue for everyone. It can happen anywhere, anytime, and can have devastating consequences.

Host Families can help to reduce incidents of cyber bullying by:

- Establishing and maintaining trust and having conversations about healthy limits for time spent online each day.
- Recognising that for many children/young people, their online life is an important part of their social identity.
- Monitoring homestay use by students and reporting to AllU any communications that may have the effect of breaching this policy.
- Implementing boundaries such as only using devices in 'safe spaces', like the living room, or having an open-door policy when children/young people use devices or computers in the bedroom.
- Reporting the cyber bullying material to the social media service where it happened.
- Collecting details of the cyber bullying material by taking a photo or copying the URL.
- Reporting cyber bullying or illegal material to AllU using AllU's **Child Safety Incident Report Form**.

Monitoring by schools

1. Schools involved in AllU's programs have the right at any time to check work or data on the school's computer network, Internet access facilities, computers and other school digital equipment/devices without obtaining prior consent from the relevant Authorised User.
2. Schools have the right at any time to check work or data on school owned digital equipment on the school site or at any school-related activity.

3. Most schools have electronic access monitoring systems which have the capability to record email and Internet use, including the user details, time, date, sites visited, length of time viewed, and from which computer or device, and therefore can monitor traffic and material sent and received using the schools' digital infrastructures. From time to time this may be examined and analysed to help maintain a Cybersafe environment.
4. Schools may deploy filtering and/or monitoring access to certain sites and data, including email.
5. Schools may from time to time conduct an internal audit of their computer network, Internet access facilities, computers and other school digital equipment/devices.

RELATED POLICIES AND SUPPORTING DOCUMENTS

Child Safety and the Child Safe Standards

Child Safe Code of Conduct

Child Safety Policy

Safeguarding Policy

Risk Management Strategy

Response to Critical Incidents Policy and Procedures

Action Plan for Dealing with Actual or Alleged Abuse

Privacy Policy

Child Protection Privacy and Information Sharing

Child Safety Incident Report Form

Photographing and Filming Students Consent Form

Cyber Safety Use Agreement

HELPFUL LINKS

<https://www.esafety.gov.au/>

<https://kidshelpline.com.au/teens/issues/bullying>

Facebook Privacy and Safety Help: <https://www.facebook.com/help/325807937506242>

Instagram Privacy and Safety Help: <https://help.instagram.com/>

Twitter Privacy and Safety Help: <https://support.twitter.com/articles/14016>

Tik Tok Privacy and Safety Help: <http://support.tiktok.com/article-categories/privacy-safety/>

Approval

Responsible Officer	Regional Manager, AIIU
Approval Body	GM, AIIU
Approval Date	30/09/2024
Next Scheduled Review	30/09/2025