Keeping students safe online at Out-of-School-Hours Learning Support Programs

Online activity, including research, social media and news feeds can be a powerful tool in the expression and protection of children's rights. Students have a platform for their voices to be shared, have quick access to huge amounts of information and can make social connections beyond their geographic community.

You may choose not to have access to the internet within your program, but if you do it is important to be aware of the risks children and young people face online in order to take steps to ensure their safety. It should also be noted that even if you do not provide internet access, mobile technology means your students may bring it with them anyway and use it during your program activities.

What are the risks?

In their publication *Working with children and young people for safety in the cyber world* (2014:10) child rights agency, Plan International Australia, categorises online risks to children in the following way:

1. Content risks

- Exposure to material online that promotes values, activities or knowledge that may be harmful or distressing to children, such as pornography, depictions of violence, hate-incitement and material promoting drug-taking, anorexia, smoking, suicide and other forms of self-harm

2. Contact risks

- Harmful communication between users, such as bullying, harassment, engaging children in online sexual talk and grooming for real life encounters that end in sexual abuse and exploitation, including trafficking or other illegal activities such as fraud and deception
- Mobile phones are a particular risk factor as it leads from virtual to real life contact more easily and can be used to track actual location of the student themselves

3. Privacy and security risks

- Identity theft, and reputational damage arising from posting content online
- A significant risk to young social network users is that they lack the understanding of the risks involved in their online activities.

4. Legal and political risks

- Possible liability for online activities, which breach national laws relating to copyright, defamation, privacy and purchase of age-restricted materials

- Involvement in monitored online political activity

5. Financial risks

- Online scams and manipulative or deceptive advertising leading to overspending on online services

If you decide to include online components in student activities a risk analysis should be conducted for your program. Not all the above risks will apply in every case, but it is good practice to consider all possibilities and assess the likelihood and possible impact of a risk eventuating. In doing this you can then ensure you have policies and procedures already in place that can reduce or even eliminate some risks as well as outline what responses are needed should an issue arise.

How to reduce and respond to risks

There are two components to ensuring your program maintains a safe environment for students using the internet – program protocols, and increasing students' knowledge of risks and ways to stay safe. Ensuring students have a high degree of age-appropriate knowledge about online safety will mean their overall exposure to online risks can be reduced, even when out of the program. Student empowerment is a key component of any safety measures.

Program Protocols	Student knowledge and empowerment
Ensure any online activity takes place in an open area, with adult supervision	Discuss with students and families why you have internet usage rules in place
Have program rules about internet usage, including how much time spent on the internet, what is okay to share online	Model good online behavior – do not accept friend requests from strangers, do not reply to unwelcome online contact, report inappropriate behavior or offensive material
Wherever possible involve families in these protocols	Discuss what risks there are and brainstorm solutions – answers that come from the students will be better suited to their needs
Ensure all volunteers and staff are familiar with, and agree to, program cyber usage rules	Encourage an open and honest approach to identifying and discussing online risks
Create passwords for all iPad and internet enabled devices which are known only by staff and tutors. This will ensure they are being used only during allocated activities.	

Engaging with families

Research by the Australian Communications and Media Authority's Cybersmart Outreach division shows that parents across Australia are keen to be involved in their children's online lives. Many parents are aware of what their children are doing online and are able to list the risks. However, older students are more likely to actively engage with their parents when they encounter an issue than primary school children. This is a concern given how active young students are online.

The Cybersmart division has five tips to encourage parents to be able to support their children's safety online:

1. Talk to your child about staying safe online and keep the discussion open as they reach new developmental stages
2. Monitor your child's time online, particularly younger children
3. Set house rules – what is okay to do and what is not, how much time is 'online' time and what kind of personal information is okay to make public
4. Consider using filters or other technological tools to help limit exposure to potentially harmful or distressing material
5. Model the kind of positive online behaviour you would like your children to use.[1]

Involving families in your cyber safety activities will support students' safety both in and outside your program. Families may not have considered risks, or be unsure what to do about them when students are required to be active online for their school work. Being able to discuss these concerns with families and provide them with tips to support their children's safety will be very valuable.

Parents who are not confident in their English language abilities may feel very disempowered when it comes to their children's online activity. Consider linking with local schools to come up with joint activities to support EAL families. Schools are allocated money from the Department of Education and Training for interpreters and translations and some will have Multicultural Education Aide who may be able to help.

With the help of interpreters you could:

- Have an open discussion with students and families about cyber safety
- Create a tips sheet together with students and families and print copies in relevant languages
- Demonstrate what students are using the internet for and invite teachers to come to this session to answer questions
- Find out about schools or community based programs that have IT sessions for EAL families, or look into running some yourself
- Ask the students and families for other ideas about how to support them.

When a student needs help

If a student who is part of your OSHLSP is struggling with a cyber safety issue it is important to provide support where appropriate. Being prepared for this is a good idea before you engage in online activities. It is important to provide non-judgemental support and to keep students connected to their friends, both online and in person, when they have experienced issues online. If a student is very distressed by something that has happened online additional support can be provided. This may be through the student's school or an external avenue such as those listed below.

- Cybersmart Online Helpline www.cybersmart.gov.au/report.aspx or 1800 55 1800
- Report content that you think may be prohibited : www.acma.gov.au/hotline

[1] Tips taken from http://www.kidsmatter.edu.au/families/enewsletter/keeping-children-safe-online

Further information

Cyber smart: Parents guide

http://www.cybersmart.gov.au/~/media/Cybersmart/Documents/Documents/Parents_guide_to_online_safety.pdf

Cyber safety training providers

https://esafety.gov.au/education-resources/voluntary-certification-scheme/find-an-online-safety-program/victoria

Cyber safety educational resources

https://esafety.gov.au/education-resources/classroom-resources

Parentlink

http://www.parentlink.act.gov.au/parenting-resources/parenting-guides/adult-issues/cyber-safety

Acknowledgement

With thanks to Louise Villanti from Save the Children for reviewing this tip sheet.