eSmart Schools

Alannah & Madeline Foundation

Keeping children safe from violence

Cyber Issues

The following list outlines significant issues children and young people face when online. It is important for teachers, parents and carers to remain aware of these issues and the potential harm that can result.

Digital Footprint/Identity the word used to describe the trail, traces or "**footprints**" that people leave online.

Geo-location software this type of software is used to identify someone's IP (Internet Protocol) address, which can reveal which country they are in – right down to city and post code, organisation and specific location. It used by law enforcement to prevent online fraud, by marketers to target advertisements, and by many mobile applications such as GPS locators.

Hacking someone who breaks into computer and network systems and performs destructive or illegal acts. 'Hackers' can also be used to quiz Internet security systems, decode and solve other technology problems.

Identity theft a crime in which an imposter obtains key pieces of personal information, such as driver's licence or passport details, in order to impersonate someone else.

Phishing when emails are sent from fake email addresses in order to deceive individuals to reveal personal information, such as passwords and credit card numbers.

Sexting the sending of sexually explicit photographs or messages, usually via smartphones.

Inappropriate content online any online content that is considered inappropriate, offensive or illegal for young people to have access to. This includes, but is not limited to, content that depicts violence, crime, racism, extremism, and sexualism. *It is important to note this type of content is often not deliberately searched for by young people.*

Hidden/Decoy apps applications that look harmless, however are designed to 'hide' content such as photos, videos, and/or text message.

Social Networking Sites (SNS) online platform that allows users to create a profile/account and interact with other users via the same platform.

Spam the sending of unsolicited commercial electronic messages via emails, instant messages, or SMS (a form of spam is 'junk email').

Grooming/unwanted contact actions deliberately undertaken by someone (most commonly an adult) with the aim of befriending and establishing an emotional connection with a child, in order to lower the child's inhibitions.

Cyber bullying occurs when technology is used deliberately and repeatedly to engage in hostile behaviour to harm someone. Groups and individuals can be both the perpetrators and targets of bullying.

Online gaming a video game that is either partially or primarily played through the Internet or another computer network.

Screen time the length of time spent using a device such as a computer, television, games console, or mobile device.

Trolling internet slang used to describe a person who deliberately antagonises people online, with the aim of starting arguments or upsetting them – most often done anonymously.

* PLEASE NOTE – Cyber Issues are not limited to this list

eSmart Schools

Alannah & Madeline Foundation

Keeping children safe from violence

Parent resources

eSmart Schools	**eSMART SCHOOLS** – www.esmartschools.org.au • Provides a detailed overview of the eSmart Schools framework. • *NEWS* tab that celebrates achievements and implementation of eSmart Schools framework from around Australia. • Subscribe to our 'Becoming eSmart' newsletter (one/term) for the latest trends, research and events about eSmart and cyber safety.
eSmart Digital Licence	**eSMART DIGITAL LICENCE** – www.digitallicence.com.au • Online challenge for children that includes quizzes, videos and games. • Encourage discussion about digital citizenship, digital literacy and digital safety between parents and child/ren. • Includes completing of 8 modules. • Fantastic tool to use as a link between school and home.
Australian Government Office of the Children's eSafety Commissioner	**Children's eSafety Commissioner** – www.esafety.gov.au • Federal governing body aimed to provide education and information about online safety. • Reporting process for cyberbullying and/or inappropriate content. • Access webpage "Games, Apps and Social Networking"
iParent	**iParent (eSafety Office)** • Comprehensive resource providing guidance for using safety settings on your family's web-connected devices. • Offers strategies for keeping young people safe online. • Download PDF "Parents Guide to Online Safety"
OpenDNS	**OPEN DNS**– https://www.opendns.com/ • Cloud-based security service for home. • No costs. • Offers filtering and security of all devices connected to home wi-fi. • Has functionality for setting parental controls.

eSmart Schools

Alannah & Madeline Foundation

Keeping children safe from violence

T.H.I.N.K

Level 1, 256 Clarendon Street PO Box 5192 South Melbourne VIC 3205
t 9697 0666 f 03 9690 5544 ABN 96 514 115 810 amf.org.au

Australian Government | Office of the Children's **eSafety Commissioner**

HOW TO REPORT CYBERBULLYING MATERIAL

1 Report the cyberbullying material to the social media service

2 Collect evidence - copy URLs or take screenshots of the material

If the content is not removed within 48 hours

3 Report it to **esafety.gov.au/reportcyberbullying**

4 Block the person and talk to someone you trust

If you are in immediate danger, **call 000** (triple zero)
If you need to talk to someone, visit kidshelpline.com.au or call them on 1800 55 1800, 24 hours a day 7 days a week

OCESC0011509

eSmart Schools

Alannah & Madeline Foundation

Keeping children safe from violence

Top Ten Tips

1	Create an 'Acceptable Use Agreement' for your families using the 3Cs to facilitate conversation – **contact**, **content**, **conduct**. Ensure that children are involved with this process.
2	Set up safe search & security controls with a platform (such as OpenDNS, NetNanny, K9) or speak with your internet service provider (such as Telstra, Optus, Vodafone, Dodo, etc).
3	Agree on where computers, laptops & mobile devices can be used in the home (such as in bedrooms, lounge rooms, etc).
4	Lights out = wifi off.
5	Agree on screen time use; decide on 'screen free' times during the day and night.
6	Get involved – show an interest in what your child is doing online.
7	Talk to your child's teacher/s and school.
8	If your child reports an issue to you, don't threaten to take away their device – this may force them to become secretive.
9	Learn how various social network/game services work. Use websites such as the 'Games, Apps & Social Networking' from the eSafety Office.
10	Tell children not to respond to any cyberbullying threats or comments online. Do not delete any of the messages – take screen shots as evidence & keep records to verify and prove there is cyberbullying.

Level 1, 256 Clarendon Street PO Box 5192 South Melbourne VIC 3205
t 9697 0666 f 03 9690 5544 ABN 96 514 115 810 amf.org.au