A Cyber Safety Champion Network has formed to support cyber safety activities in Queensland Anglican Schools.

The Cyber Safety Champion Network is a network of professionals who share:
- an interest in school cyber safety activities;
- ways of working on cyber safety;
- solutions to cyber safety concerns; and
- ideas and good practices.

The network also functions to lead and support organisational change for cyber safety quality improvements, to establish first points of contact to expediently receive and disseminate cyber safety material and to assist in the establishment of shared resources for Anglican schools. By working together, the network aims to support each other in developing strong, innovative and improved practices.

The Cyber Safety Champion Network is chaired by the ASC Cyber Safety Support Officer and each school has been offered the opportunity to nominate a Cyber Safety Champion to represent their school in the network. Cyber Safety Champions are nominated by the school because they fulfill important roles in driving the school’s cyber safety quality improvement agenda and efforts (eSmart Schools planning, implementing and sustaining).

Speak to your Administration and find out who your school’s Cyber Safety Champion is.

The Anglican Schools Commission has devised a framework, and acronym, to assist parents to trouble shoot concerns around device use and assist their child in the digital world. This frame is called the AIDE Principle: Application, Internet, Device, Educate and Engage. Contact your Cyber Safety Champion to express your interest in attending a Parents AIDE session. Sessions run for 1-1 ½ hrs and are followed up by a drop-in Q&A session (usually the following day or week). Learn more about tailoring your online security or settings to the capabilities of your child.

It is also important to assist young people to develop positive online behaviour, as accessing inappropriate material may lead to psychological harm and reinforce negative behaviours. At times your child may have unsupervised access on smartphones, game consoles and other devices. Taking an interest and discussing what they are doing helps you to be involved and lay the foundations for safe online behaviour and culture.

Here are some handy links

Dealing with age appropriate content
7 ways to Manage Devices
iOS Restrictions & Parental Controls
Google Play Restrictions & Parental Controls
Microsoft Windows Family Accounts Set up
Set up Apple Family Sharing

Minimise cyber risks that come with sharing images and videos online. Always remember that some people will view images or use them differently from what you intended. The eSafety Commissioner has reported images have been harvested from social media and students placed at risk as they can be identified by details in their photos.

Before you snap!
- Is the photo going to offend anyone?
- Who is going to see the photo?
- Who else is in the photo?
- Some people will not want their image shared.
- Are the people and places in the photo able to be identified?

What is in the background?

Do not send photos:
- containing personal details (i.e. names, school or tag)
- may be interpreted as offensive or demeaning
- may harm another’s reputation or embarrass them
- show any children in distress

Limit geo location tagging
- Photos may send the GPS coordinates of where they were taken
- Before posting images check both the App settings and Devices settings to turn off or limit sharing details.

Click for more information
eSafety: photos & social media
Institute of Families: Good Practices
eSafety: Young and Safe

Protect your personal information from being taken over online. Even though legitimate businesses may need your details others might misuse your personal information for their gain. Be smart and consider how and with whom you share your private information:

- Keep your devices up to date
- Update passwords regularly (don’t use pet names)
- Lock down your social media and increase your privacy settings
- Read App user agreements. Competitions often use your data for marketing and advertising. Check your spam filtering software is up to date.
HELP

Your choices define not only your online reputation but also how people see you in real life. Adding or responding to haters, flammers (hostile and insulting people), trolls (malicious people who try to provoke you) or fakers may have real world consequences.

I am responsible
I question things
I respect differences

As a rule of thumb if you think at any stage ‘I could get in trouble’ - do not send. The ‘Online THINK and SPACE’ guidelines (below) may help you decide what to do, regardless of whether it is written post, an image or video.

THINK before you post online
Would my Grandma be ok with this?
T: Is this true?
H: Is this hurtful?
I: Is this illegal?
N: Is this necessary?
K: Is this kind?

SPACE give yourself some space and just pause. Remember:
S - Stop: You don’t have to post anything.
P - Pause: Get up and walk away...the longer the better.
A - Assess: THINK what will happen if you post it.
C - Check: Talk to a responsible adult. What do they say?
E - Execute if it passes, otherwise DELETE!

Hints to dealing with online mayhem
1. Don’t feed the trolls and haters. They only want to upset you. Ignore them.
2. Respond to good behaviour only.
3. Use the forum’s Report buttons for bad behaviour.
4. Take a break and walk away.
5. Talk to a responsible adult - offline.

SOCIAL MEDIA: 10 GOOD RULES

Social media can be great way to be connected to family, friends and what’s happening online. However, we need to make sure we understand the basics, so social media can complement and not overtake the REAL world around us:

1. Rules in real life apply to you online. You can’t defame people or threaten people. The internet isn’t as anonymous as most think so don’t pretend to be someone you’re not. You will be held responsible for what you post.
2. Do unto others as you would have them do unto you. If you wouldn’t say it to their face, then don’t do it online.
3. Play nicely. Your online interactions are a reflection of you and will follow you around (maybe for years). Be positive and encouraging to others. Make yourself a positive person to be associated with and people will want to stay connected.
4. Don’t post when you’re angry. Don’t say something that you will later regret. If you’re upset, use SPACE and THINK to help process what’s happening (see help section).
5. Consider that posting is publishing forever. If you’ve posted it, it can be tracked back to you. When you post things online, you’re creating a digital fingerprint. Consequences can include losing your job, facing criminal charges and public disgrace.
6. Use different usernames and passwords. Don’t use the same username and password for all of your emails or sites you visit. If someone figures out your password or security answers, they’ll have access to everything. It’s best to set-up different usernames and passwords and two factor authentication when available.
7. Your usernames and email addresses reflect on you. You may need to use your email address for university applications, job applications and resumes. Does your username and email address make a good impression?
8. Don’t react too fast or be too quick to judge. Take a breath and relax. Show patience and wait. Have you interpreted the words wrongly? Has the intent of the message been lost or has the sender been unable to express themselves correctly? Take the time to re-read the message. Don’t assume everything is malicious, often translation can read two ways.
9. Don’t reveal confidential information in chat rooms. You may think you know the person on the other end of your chat, but he/she can be catfishing (a fake account pretending to be something they are not, this includes gender). Don’t give out your confidential information online, such as your full name, home address, phone number or names of family members.

10. Balance your time and have an exit plan for EACH session: Plan time for using social media. Set your goals for what you are going to do and how long you are going to be online. Understand that constantly checking your social media/devices also breaks your concentration and does not let you focus on real world issues.

If you are worried or need further information, talk to your parents, your teacher or another responsible adult.

Kik is marketed as a smartphone messenger app for those aged 13+. The app is available for most smart phones and tablets (including iPods). The app allows users to send and receive texts, photos, images, GIFs and videos via your existing Wi-Fi connection or data plan. Due to the potential for exposure to inappropriate material and unwanted contact from adults, Kik is potentially an unsafe application for use by school aged students. Kik is often overlooked by parents as a simple text app, however, for several reasons it isn’t: users can create accounts anonymously; the app does not require age verification; it has built-in web browsing capability; and it allows users to converse in closed groups and to direct message. To learn about how to protect privacy on Kik, how to block users, and how to make reports click here.

APP BITS

Click for more: Report Cyberbullying Making a Complaint Cybersmart challenge

Minecraft

The new update is out, allowing thousands of iOS, Android, PC, Nintendo and Xbox One players to all play together at one time. The new update requires all users, regardless of platform, to create a free Xbox live account to play online. Parents can set up online safety and privacy settings (click here). After connecting to multiplayer you can mute chat, in settings, to allow a user to play but not be exposed to any chat. Parents can limit multiplayer interactions to friends only or even turn off multiplayer access. Beware the update also has a game store in which children can purchase coins costing real money from $3 to $31 (if an account is connected).

Click for more: Bullying No Way Kids Helpline Report Cyberbullying

Anglican Church of Queensland

10 things parents should know about Minecraft Xbox live online safety and privacy settings