



Student Online Safety

Cairnlea Park Primary School recognises the educational value of digital technologies – including the internet – to support students’ learning.

In particular, the internet provides access to valuable educational resources. Students can use the internet for:

- Research, collaboration and communication
- On-line educational sites (such as Mathletics, Reading Eggs, BrainPop)
- Blogs, wikis and other Web 2.0 tools to support curriculum programs.

We also recognise **the need for students to be smart, safe and responsible users of digital and online technologies.**

Common cybersafety issues for children include cyberbullying, accessing or sharing inappropriate content and protecting their personal information.

To address this, Cairnlea Park Primary School:

- provides classroom cybersafety sessions to explicitly teach students about smart, safe and responsible online behaviours
- uses filters to block access to inappropriate internet sites when students are connected to the school network
- blocks access to social media platforms when students are connected to the school network
- has policies for the Smart, Safe and Responsible Use of Digital Technologies and for the use of Social Media
- provides an online “Share A Concern” system where students can confidentially report any online issues to the school’s Student Welfare Team and ICT Team.

Teaching children to be cybersafe will enable them to navigate the online world safely and responsibly, and can help to protect them from online risks. This is **best taught in partnership with parents/guardians**. We request that parents/guardians work with us and encourage this behaviour at home.

Internet Restrictions

Most online and cybersafety issues occur when students access the internet and social media platforms outside of school. This can include using computers, iPads/tablets, smart phones and gaming devices such as an xBox, Playstation, Wii, etc.

Parents need to be aware that **school internet filters** (which block access to inappropriate internet sites and to social media sites) **only apply when students are connected to the school network**.

Whenever students connect to the internet from their home networks, it is very likely that they will have “unrestricted” internet access – unless parents specifically apply their own restrictions or filters.

Supporting Your Child Online

To support student online safety, parents may consider the following.

- Have open conversations and reassure children about their internet use. Let them know that you will not deny them access to the internet if they report feeling uncomfortable or unsafe when online – this is a very real concern for children that may stop them from communicating with you openly.
- Be aware that most social media services and apps (such as Instagram, Snapchat, Facebook, Twitter) require users to be 13 years old to join. Parents should be involved in any social media activities of their children.
- Agree on daily screen-time limits and plan screen-free time (eg time for outdoor play, music, sport, reading).
- Set tech-free times and zones at home (eg no devices in bedrooms, no devices after 7pm).
- Create a Family Technology Plan (in consultation with your child). Your plan could cover things like screen-free areas in your house, internet safety rules like not giving out personal information, and programs, apps and web sites that are OK for your child to use.
- Lead by example (reduce your own screen time).
- Participate in tech-free activities with your children.

Parents are encouraged to discuss with their children the possible implications of inappropriate internet use. In order to protect themselves – both online and offline – young people need to consider how they manage messages, images and information.

- Talk to your children about **managing personal information** on social networking sites. Encourage them not to put any personal information on their profiles. This includes their full name, home address, phone number, personal email address, or the name or address of their school.
- Reinforce with your children that they should **never text, email or post anything online that they would not say out loud** in front of parents or teachers.
- Encourage your children to **be careful when they post or share photos** and to **consider that what they share may be viewed by others**. A good general guide is for kids not to post photos that they would not want strangers to see.
- Remind your children that **much of what they do online can be made public**, and may go beyond the group of friends they intend it to reach.
- Be aware of age restrictions and content of online games and social media platforms.
- Talk to your children about the potential social, academic, employment and legal implications of posting inappropriate material of themselves or others online. Encourage them to think about who might see the content and what the impact might be, now and in the future.
- Remind them to **also respect other people's privacy and reputation**. They should not post images of others without their permission and should take care with comments about others.

Parental Controls and Responsibilities

**At home, parents need to be responsible for
the online safety and interactions of their children.**

The use of **parental control tools** can help parents keep their children safe when using devices and the Internet at home. Many different tools are available and they all offer different functions.

Most parental control tools can:

- allow or block specific websites or applications (i.e. programs or games)
- restrict chat features
- filter different kinds of content (such as sexual content)
- set screen time limits (handy if you are not home and want to limit the time your child spends on a game or social media)
- block in-app purchases
- block numbers and SMS
- allow parental monitoring.

Parental control tools are available for most devices. Some are settings or options that are included on the device (which need to be activated). Others are free or paid commercial software that needs to be installed on the device.

- **Parental control tools** and **safety options** are available for iOS devices (iPads & iPhones) and Android devices (other tablets & smart phones), as well as many gaming consoles.
- Apple computer systems and Microsoft Windows computer systems both **offer family restrictions and monitoring tools**.
- YouTube and YouTube Kids have a **safety mode**; Netflix and Stan offer **age-based settings**.
- **Safe search settings** are available for Google Safe Search, Google Chrome and Yahoo7.
- Many internet providers (eg Telstra, Optus, iiNet) provide **parental control tools**.

However, **it is essential to note that no parental control tool is completely effective** (especially at filtering content within social media sites).

It is important to understand the nature of children's online activities, and to talk to them about staying safe online and being aware of the behaviours of themselves and others.

The Australian Government's Office of the eSafety Commissioner provides information about parental controls at:

<https://www.esafety.gov.au/education-resources/iparent/online-safeguards/parental-controls>

A review (from the UK) of *The Best Parental Control Software of 2018* is available at:

<https://au.pcmag.com/parental-control-monitoring-products/44998/guide/the-best-parental-control-software-of-2018>

Further Resources for Parents

There are many online resources to support parents in managing the online activities of their children. Some of these are:

Office of the eSafety Commissioner (www.esafety.gov.au)

- **iParent** - where you can learn about the digital environment and how to help your child have safe and enjoyable online experiences.
<https://www.esafety.gov.au/iparent>
- **Parents Guide to Online Safety** – a booklet with practical, issue-focused information and advice for parents of children of all ages. Includes topics about Cyberbullying, Social networking, Inappropriate content, Online safeguards.
<https://www.esafety.gov.au/about-the-office/resource-centre/brochure-parents-guide-to-online-safety>
- **Safe Social Networking** – How can I support my child to be safe on social networks? Being involved, Age guidelines, Personal profiles, Privacy, Respectful communication.
<https://www.esafety.gov.au/education-resources/iparent/staying-safe/social-networking/safe-social-networking>

DET Bully Stoppers – Parents and Cybersafety.

(<https://www.education.vic.gov.au/about/programs/bullystoppers/Pages/parentcyber.aspx>)

The Australian Parenting website – Pre-teens entertainment and technology.

Articles on Cyberbullying & internet safety, Screen time, Digital life.

(http://raisingchildren.net.au/entertainment_technology/pre-teens_entertainment.html)

Janell Burley Hofmann – international author, speaker and consultant working with youth, parents, educators and professionals; founder of iRules Academy and the Slow Tech Movement.

iRules, Parent Tech tips – ideas for family technology plans or “contracts”.

(<http://www.janellburleyhofmann.com/irules>)

Student Wellbeing Hub – Parents Info & Advice – Primary – Being Safe Online.

Resources for parents about various online safety topics.

(<https://www.studentwellbeinghub.edu.au/resources#>)

Digizen – provides information to raise awareness and understanding of what digital citizenship is and encourages users of technology to be responsible digital citizens. It shares specific advice and resources on issues such as social networking and cyberbullying.

(<http://www.digizen.org/>)