Suncoast Cyber Safety
Parent Guide
Mission Statement

Suncoast Christian College exists to provide Christ-centred education that promotes life-long learning, develops excellence and Christian character, and fosters social responsibility.
Introduction: Why Cyber-Safety?

We live in an increasingly technologically rich world. The advent of information communications technology has opened up a new world of information and experiences allowing people to meet, interact and communicate with people from across the world. These activities are especially appealing to young people. Students are increasingly online, connected and active in this new world. Chatting, blogging, emailing and social networking are intrinsic to their world and provide a new means of communication. Some of the key activities that young people engage in online include:

- Social Networking
- Communicating - Chatrooms, Instant Messaging
- Texting and use of Mobile Phones
- Web Surfing
- Downloading
- Gaming

Whilst many of these activities allow for positive experiences, there are risks associated with the misuse of these technologies. These include:

- Exposure to inappropriate content
- Physical danger
- Harassment and bullying
- Viruses, worms, trojans
- Unsafe communities
- Copyright and plagiarism

The safety and wellbeing of young people is of paramount concern to parents, guardians and educators. The challenge is how to teach students the relevant skills so that they can navigate the Internet safely and effectively. For many adults, understanding and keeping up with their children in this area is challenging. Given that the proper use of information communications technology should be the joint responsibility of parents, guardians and schools, this booklet has been produced to provide you with an overview of the main risks associated with the Internet. It is hoped it will also provide strategies that may be useful in helping your children make safe and responsible choices online.

Overriding Common Sense

Let’s get the obvious out of the way first, before we move onto a more detailed discussion of some of the different risks. The most important thing parents can do is to establish rules for where, when, why and for how long young people will be online.

Online activities should take place in a public area of the house where there is regular supervision and parents are aware of what is going on. Be proactive, be involved and be aware.
Social Networking

Social networking sites (SNS) are like virtual communities, providing a social lifeline for today’s youth. Sites like Facebook and Tumblr allow users/members to create an online profile or web page. Members can then post personal information, photographs, blogs, music clips and other information about their interests online. A big part of customising their space is to upload photos, images and personal information. Most sites also have a blog where users can write their thoughts, encourage others to join in and post comments.

What are the dangers?

Social networking sites hold significant appeal for young people. Whilst such sites provide opportunities for self-expression and identity formation, they also pose risks. These include:

- Posting inappropriate content. Risks arise when young people give out information that is too personal or allows others to know who they are or where they live.
- Exposure to anti-social or illegal material.
- Being targeted by sex offenders.
- Cyber bullying.
- Sending/receiving hurtful or inappropriate messages.
- Identify theft - many people within social networking sites encourage users to join their space or view their profile by encouraging them to click on links that ask for username and passwords. This allows others to gain access to their passwords and other private information.
- Social networking can be very addictive and it is easy to waste a lot of time, so that other activities, tasks, chores and study are neglected.
- Living a fantasy – for some people blogs provide an opportunity to “invent” a life or an image of themselves online. The way a young person constructs their online identity may reflect their self-esteem and the ways people respond to it may have a serious impact.

What can you do?

- Encourage them to limit friendship links to known friends only. Young people should never accept friend requests from mere acquaintances, friends of friends or people they only think they know. The parent or guardian should check the list of “friends” their child has accepted from time to time.
- Ensure computer use occurs in a “public” space in the home where use can be monitored. Set clear time limits for this type of activity or use as a reward once other tasks are complete.
- Encourage children to only upload pictures that you as their parents/guardians would be happy to see.
- Make sure they don’t put any personal information on their profile such as phone number, personal email address, home or school addresses or other personally identifying information.
- Ask them to show you how to use a social networking site - getting involved will empower them to share the experience with you.
- Ensure they set their profile to private - but emphasise that a private profile is still public. Nothing on the internet is private or protected.
- Regularly review your child’s profile.
- Make a plan with your child for what to do in the event of cyber bullying or transmission of inappropriate material—e.g. report to parent immediately; don’t respond back; parent to keep a copy of bullying or offensive materials for reporting to school or police; block offenders.
Communicating Online: Chatrooms

The Internet allows people to communicate in a multitude of ways. Online communications are popular with today's youth as they allow for real time (instantaneous) communication. Chatrooms provide one of the easiest ways to communicate online. Chatrooms can be accessed on mobile phones as well as computers and other online devices. A chatroom allows people with similar interests to meet and communicate together by typing messages on their computer. These text messages can then be seen immediately by everyone present in the chatroom. You can watch without joining in, or you can join the conversation at anytime. As well as being able to contribute to a conversation it is also usually possible to chat one on one with another person. Some chat rooms allow for voice and video chats. This enables you to hear and see others and vice versa.

For young people, the attraction of chatrooms are that they allow them to be whoever they want and provide opportunities for experimentation and expression with less inhibition and more risk taking. Fortunately, many chatrooms have rules that they require users to follow. Some of the chat rooms designed for children are monitored and there are rules against offensive language, violence and other negative issues. However, as this is not always the case, it is important to be aware of the types of chatrooms young people are entering.

What are the dangers?

- The content of chatrooms may not always be appropriate. Young people can find themselves in situations where they can feel out of their depth. They may be exposed to explicit sexual talk, inappropriate language and ideas.
- It is easy to be anonymous in a chatroom. People are not often who they say they are and it is easy to adopt a false identity.
- Leaving an inappropriate digital footprint. Some children may be encouraged to give out personal information or send photographs of themselves.
- Harassment - Young people might encounter messages via chat that are demeaning, offensive or abusive.
- Time wasting – time “flies” when chatting online and it is easy to spend an inappropriate amount of time chatting instead of doing your work.

What can you do?

- Talk frequently to children about their experiences in chatrooms and the types of chatrooms they are using.
- Agree together on the chatrooms that you deem acceptable for use and the rules of engagement (e.g. is it okay to talk to people who are not personally known to the young person).
- Encourage them to discuss any inappropriate content or problems they may have experienced – again, make a plan of action should this occur. The young person should know exactly what to do in this instance.
- Discuss stranger danger and strategies to avoid giving out personal details.

It is important to be aware of the types of chatrooms young people are entering.
Communicating Online: Instant Messaging

Instant messaging is another popular way of chatting. Often known as IM, this involves two or more people being online at the same time. It differs from chatrooms, because the people involved can only chat to those who are on their contact list. Young people often feel that they can talk more intimately in this environment, and often use their own text style language to do so. Although IM uses the user’s own contact list, young people still can chat to strangers whom they have “friended”. Facebook includes a “chat” feature which is a form of Instant Messaging.

What are the dangers?

- IM is a very intimate form of communication - more so than a chatroom and therefore predators will often use this as a means to extract personal information from a young person.
- Private conversations can be started with anybody (including strangers) with many instant messaging programs.
- Instant messaging provides the opportunity to release personal information in real time.
- Once people have created their accounts they can start sending messages from any computer connected to the Internet which also has the instant messaging programs installed. This makes supervision more challenging.
- Instant messaging can be very addictive and time consuming and can get in the way of other activities.
- Instant messaging can be the cause of significant disruption to study or work time. Students may not have uninterrupted and extended study time and may therefore not have the opportunity for deep thinking. This will ultimately affect their academic performance.

What can you do?

- Talk to children about their use of Instant Messaging, such as who their IM buddies are and how they met.
- Talk about what they are to do if they are approached by an unknown person, never to give away any personal information.
- Maybe even consider disabling a Facebook or IM account during term time.

IM is a very personal form of communication.
Mobile Phones
The use of mobile phones is increasingly prevalent amongst young people as the main device for making phone calls, as well as texting, social networking and sharing photos. Data enabled phones allow users full access to the Internet. The appeal of mobile phones to youth as an important tool for social interaction has provided a lucrative market for the mobile telecommunications industry.

What are the dangers?
Mobile phones present several concerns.
- Increasingly cyber bullying and sexting occurs via mobile phone technology as these devices are largely unsupervised and make these activities all too easy.
- With the advent of picture and video messaging - young people need to be increasingly careful about the images they share.
- Another primary concern raised by parents and academics is that mobile phones are encouraging youths to communicate through technology rather than face-to-face.
- The 'always on' nature of mobile services means that risks such as bullying, people making inappropriate contact and the chance that children will access unsuitable content are always present. Sleep deprivation is a growing problem as many teenagers experience limited or broken sleep because they are staying up late or waking through the night to respond to messages through social networking apps.
- Young people also need to be aware that they put themselves at risk of mobile bullying, or inappropriate intimate contact if they give out their mobile number to people that they don’t fully trust.
- Running up an unexpectedly large mobile phone bill through calls, texting or data usage. This is particularly the case with data charges for the use of internet and email on mobile phones, which are not always clearly understood by customers.
- Breaking the Law – young people must understand that the use of this technology is covered by the Telecommunications and Privacy Acts. Improper use may result in the police becoming involved – for example use of the phone for harassment; recording and publically display images of people without their permission (e.g. on YouTube); theft and unauthorised use of a SIM card.

What can you do?
- When buying a mobile phone, consider what services are available on it. A large proportion of mobile phones have web access. This means that young people can access unfiltered content from the internet wherever they are and without parental or teacher supervision.
- Talk about appropriate and lawful use of the mobile phone - use of mobile cameras, downloads, sending photographs, texting.
- Make an agreement about the purpose and use of the mobile phone.
- Remind your child that any image they send on their mobile can be changed and shared online, and that once they have sent an image they have lost control of it.
- With more young people having Internet-accessible mobile phones, the question of monitoring becomes more complex. Mobile phone use is difficult to monitor other than by the monthly charges, because they are so small and portable.
- Use a pre-paid system, rather than a monthly plan where the user can overspend.

Make an agreement about the purpose and use of the mobile phone.
Computer Games

Computer games are a significant part of many students' lives and a form of entertainment that many could not do without. Gaming can be great fun, providing a place where young people play and chat to each other. There are a number of different types of games but the most popular seem to be the multiplayer games or (MMORPG's) that are played online. In multiplayer games, players either compete against each other, or team up to achieve a common goal such as defeating an enemy that can consist of either computer or human players.

What are the dangers?

Recent research is indicating some potentially worrying consequences for people involved in excessive gaming due to the link between gaming activities and release of the pleasure chemical endorphin in the brain. In some instances, excessive online gaming can be addictive for young people and lead to a numbing of a person's emotions. Some young people can become so involved in gaming communities that they lose touch with the real world. Parents need also be aware that online gaming can be used as a means of grooming children.

What can you do?

- Limit gaming sessions to no more than 45 minutes per day
- Play games with your children.
- Research suggests that parents who actively engage in games with their children are more aware of what's going on with their children's development and interests.
- Negotiate and set time limits for gaming with agreed consequences if children breach this.
- Let them play as a reward for finishing homework.
- Always check games ratings before you buy. Australia's ratings and classification system for games are useful in helping parents decide what is appropriate. (http://www.classification.gov.au)

Computer games, while entertaining, can be very addictive.
The Internet and Inappropriate Websites

The Internet and World Wide Web are integral to the lives of children of all ages, connecting them to an almost limitless source of information. It is easy to use with users being able to move quickly from one page to another through hyperlinks. The Internet is not moderated or censored in any way and whilst this may provide advantages in some instances, it also provides many disadvantages.

One of the main problems for students is how to find useful information. An understanding of how searching or surfing the Internet works is important in reducing the amount of inappropriate information students are exposed to. Most students use search engines, like Google, to find things on the Internet. There are many other search engines available, such as Yahoo, all of which are popular with students. Nevertheless, students must be able to develop effective search strategies in order to minimise the time spent searching and the amount of offensive material they may find.

What are the dangers?

Exposure to inappropriate material that is potentially harmful is one of the risks posed by searching the Internet. While a lot of the material found on the Internet will be fun, educational or informative some of the content may be upsetting or cause distress. Even without trying, children can come across materials that are obscene, pornographic, violent, hate filled, racist, or offensive in other ways.

What can you do?

There are a number of ways that young people can search safely. It is important to remember that the more accurate their search, the more relevant the search results will be and the less likely that unwanted results will be returned. Critical thinking skills are the key to keeping young people safe online. Such skills are transferable and portable and can be applied when they are in situations away from the filters on school and home computers.

Parents can help their children in a number of ways:

- Make sure children know what to do if they come across inappropriate content and that they feel safe to report it promptly to the parent/guardian.
- Make sure your children understand what you consider appropriate for them. What kinds of sites are they welcome to visit? What areas are off limits? How much time can they spend online?
- Make online exploration a family activity. Use the computer in the living room or family room. This arrangement involves everyone and helps you monitor what your children are doing. This is particularly important for younger children who do not have the maturity to deal with certain materials.
- Explore the various types of search engines and how they work. Many of the main search engines will allow users to conduct safe searches. This means that they will filter inappropriate material.
- Show children how to use and evaluate information. Not all information is reliable or trustworthy.

Safe searching

The Sunshine Coast Library website (http://library.sunshinecoast.qld.gov.au/) provides access to many ‘safe’ sites for students to use when doing homework or research.

Much of the best information for assignments is not available on the open Web. The College and Sunshine Coast libraries subscribe to “Reference databases” which contain information from reliable sources that have been reviewed and edited. These databases can be accessed by the students via the library section of the Suncoast Intranet or via the Sunshine Coast Libraries website. All of these databases contain safe, useful and relevant information for students.
Cyber Bullying
Cyber bullying has become a major issue for the youth of today. Cyber bullies take advantage of young people's reliance on technology and use it as a means for spreading harassing and harmful messages. Cyber bullying is defined as bullying which is carried out through technology such as social networking, instant messaging, email or other Internet services. It certainly includes bullying through mobile phone technologies such as short messaging service (SMS).

Examples of cyber bullying include:
- Teasing and being made fun of.
- Spreading of rumours online.
- Sending unwanted messages.
- Sharing someone's secrets or private information online.

What are the dangers?
Cyber bullying is likely to cause significantly more harm than traditional forms of bullying. This is because:
- Online communications can be particularly nasty and vicious.
- There is no escape. The bullying can take place 24/7.
- The bullying material can be distributed to a world-wide audience and is often irretrievable.

What can you do?
- Discuss cyber bullying with children and any problems they may have. Have an action plan – the young person should know exactly what to do in the event of a cyber bullying incident.
- Watch out for any behavioural changes especially as they relate to online behaviour. Often problems that exist in the real world will find a way to the Internet.
- Know who to contact if your child is being cyber bullied and what the procedure is for removing content from the Internet. Most reputable sites will have a Contact Us or Complaints section on their website.

*Cyber bullies take advantage of young people's reliance on technology.*
Protection Technologies

Internet content filters can help manage the online environment that students use. Filters help to reduce the risk of young people coming into contact with material that is offensive, upsetting or dangerous. Internet content filters offer many different functions that help to block, screen or monitor unwelcome material. However, it is important to remember that some children may learn how to bypass filters. There are many websites dedicated to showing them how to do this.

All school laptops are protected by Netbox Blue at home and at school. Netbox Blue provides a very high standard of protection against pornography, spam, hacking, hate, drugs, phishing, fraud, spyware, malicious and anonymizer (proxy) sites. It takes a cautious approach in regard to an unknown site, blocking it until the software has investigated the site’s credentials and ensured it is safe for student browsing. This process usually occurs within 15 minutes.

Each laptop has a protector agent which monitors internet activities at home and applies the College internet policies to the laptop wherever it is being used and regardless of the user. It works with both Windows and Mac operating systems. In addition to URL filtering, Netbox Blue also offers content filtering, which means that it is able to block inappropriate language in search engines and social networking sites such as Facebook.

Netbox Blue monitors chat on social networking sites and prevents the use of restricted language (swear and inappropriate words) both to and from laptops which have the filter installed. It also does this for words typed into search engines, such as Google, and enforces the safe search policy of those websites. For example, students can’t turn off SafeSearch, which is Google’s own automated method to prevent adult or objectionable content from appearing in search results.

Whilst the network, software and operating system filters will assist in limiting access to inappropriate material, computer software will not replace the supervision and care of a parent. Good advice is available from the Federal Government website, http://www.cybersmart.gov.au/

Notebook use, particularly for younger children, should be restricted to family areas of the home, such as the family room or kitchen. This is particularly important where a wireless access allows internet use throughout the home. Unfiltered Internet use behind a closed bedroom door is strongly discouraged.

The College strongly endorses the Cybersafe 247 product for use in homes for the effective management, control and filtering of the Internet use for all Wi-Fi enabled devices. More information is available through the company website: http://www.cybersafe247.com
Computer Viruses, Worms and Trojans

Viruses, worms and trojans are malicious programs that can cause considerable harm. Computers can become infected with any of these when connected to the Internet, sharing storage devices (like USB sticks), downloading and opening infected email or visiting dodgy websites such as some gaming sites. It is important that computers are protected from these risks by software and that common sense is used. Notebook computers provided by Suncoast are protected by Total Traffic Control anti-virus software.

What is a Computer Virus?

A virus is a computer program (usually disguised as something else) which is designed to cause undesirable effects on computer systems. Viruses are often designed so that they can be transferred from one computer to another without the users knowing. They can be hidden in e-mails, on CDs or in files that are shared across the Internet.

Computer viruses can cause harm to computer systems and need to be avoided. Computer programmers called hackers often use viruses to stop or slow down computer systems.

How do I stop a Computer Virus?

The best way to protect your computer from a virus is by installing virus protection (anti-virus) software. All College computers are protected by Kaspersky Lab software.

This software scans your machine (usually when you start it up), locates and removes any viruses that are found. Viruses can be transferred to your computer without you knowing. Popular Internet activities such as reading email or surfing the Internet can lead to your machine becoming infected. Viruses can also enter directly via computer disks or other storage devices that are connected to your computer.

It is important to upgrade your virus protection software regularly as new viruses appear every day. College computers will update automatically when connected to the school network.

Where can I find anti-virus software for my home computer?

A good place to start is by talking to your Internet Service Provider (ISP) about what solutions they offer. They may be able to provide virus protection as part of your account with them.

Virus protection software can be purchased from local computer stores or downloaded directly off the Internet. Sometimes they are bundled in with other software such as content filters or parental monitoring software.

To promote the use of virus protection software, the Internet Industry Association (www.iia.net.au) has set up a national initiative. More information can be found at: www.secureyourcomputer.info

What is a Worm?

A worm is a type of virus (computer program) which takes control over computers. The worm’s aim is to replicate itself so that it consumes all resources of a personal computer or large computer systems and networks. Because of this intensive replication, worms can slow down the speed of the Internet.

Installing virus protection software is an important step in preventing or removing worms from your computer.

What is a Trojan?

A trojan is a program installed on computers usually without the owner’s permission or knowledge and is used to gain access by unauthorised people to the computer. Trojans appear to be safe, but they often hide malicious computer code that can spread a virus or worm. Trojans can sit harmlessly on a computer until the hacker activates it and gains access.
Challenges for Parents: How Can You Help?

Whilst young people are increasingly techno-savvy they still need parents, guardians and educators to teach them how to make smart choices about whom and what they find online. Here are some tips to help you guide your children's experience online:

1. Explore cyberspace yourself, be aware and involved. Learn enough about the Internet and other information communication technologies so you can talk about them.
2. Show an interest in what your child is doing online and where they are going.
3. Use the computer in a public shared space at home - not a bedroom or in a place where monitoring and supervision is not possible.
4. Investigate filters and monitors.
5. Set rules for computer use - this may include how much time is to be spent on the computer for study and recreation, where it is to be used and so on.
6. Help children view online information with a critical eye. As young people are not only viewing content on the Internet but contributing to it, it is important that they are able to think critically and evaluate what they post, read and see.
7. Find out how much time your child is spending online. Ask yourself if your child's internet use is affecting their school performance, health, and relationships with family and friends.

Five key online safety principles

Most people behave reasonably on the Internet. However, there are some who don't and it is important for children to be aware of how to deal with these people when online. Teach your children that they should:

- **Never** give out personal information of any kind.
- **Never** share their password, even with friends. Their best friend today may not be their best friend tomorrow.
- **Never** arrange a face-to-face meeting with someone they meet online.
- **Never** respond to messages that make them feel confused or uncomfortable. They should ignore the sender, end the communication, and tell you or another trusted adult right away.
- **Never** use bad language or send mean messages online.
Useful Websites

Cyber smart

Address: http://www.cybersmart.gov.au/
Cyber smart is the Australian Government's internet safety initiative which consists of a wide range of activities. Together, these activities provide a comprehensive response to the needs of the Australian community in protecting their families online. Has particularly relevant information for parents.

Whilst young people are increasingly techno-savvy they still need parents.