



#### Dear Parent/Guardian.

Welcome to the St Bede's College Cyber Awareness Night. We name this night as "Cyber Awareness" rather than "Cyber Safety" as the issues regarding ICT Devices now greatly extend beyond safety into issues of personal well-being and academic achievement. The documents in this booklet are a starting point only. Links directing you to many additional resources are listed within this booklet. In particular, the website of The Office of the eSafety Commissioner (www. esafety.gov.au) has a wealth of information. Please spend the time to explore this site and contact me if you have further questions.

Mr David Cracknell
Deputy Principal - ICT and Infrastructure

## Contents Page Cyber Awareness Evening

#### Page 3

Useful Links - Some helpful links to some of the resources talked about during the session.

### Page 4 & 5

iParent from eSafety - Learn about the digital environment and how to help your child have a safe and enjoyable online experiences

#### Page 6 - 11

Optus Digital Thumbprint - teaches the advantages of a positive online presence, through free in-school workshops, in a fun and interactive way.

### Page 12-13

Circle with Disney - The smart way for families to manage content and time online, on any device

### Page 14 - 17

Apple App Limits and Downtime - Learn about how to use Apple's new Downtime and App Limits on IOS 12.

#### Page 18 - 19

St Bede's College ICT Protocols and Acceptable Use.













**Useful Links**Cyber Awareness Evening

eSafety - iParent https://esafety.gov.au/iparent

Optus - Digital Thumbprint http://www.digitalthumbprint.com.au

Circle - With Disney https://cybersafehouse.com Promo Code: SBC2018

Family Zone https://www.familyzone.com





### Screen Smart Parent Tour: facts and tips

#### Social media

Fact: On average, children aged 10 to 14 years have 2 active social media accounts<sup>1</sup>

- 1. Talk regularly with your child about privacy settings on social media. Updating your own privacy settings sets a great example and helps you understand potential safety issues. Be aware of any minimum age requirements.
- 2. Keep your ears and eyes open. Other parents and the media can be a great source of information when it comes to the latest or most preferred app.
- 3. Let your child know that you're really interested in how they're connecting with friends. They might be more inclined to talk openly about social media if you talk about what others (their friends and peers) are doing online.

#### Screen time

Fact: On average, outside of school, 10 to 14 year olds spend 23 hours online per week<sup>1</sup>

- 1. Try to encourage positive screen time, like content that you can view and enjoy together. Discourage anything that is overly aggressive or disrespectful.
- 2. Negotiate key rules together, such as when screens can be on and when they need to be turned off. Young teens are likely to respond better to rules that they've contributed to and see as being fair and consistent.
- 3. Agree ahead of time on the rules and strategies to get your child to switch off from the screen. With gaming, think about a timer that signals that game time is nearly over and be clear about the consequences for not switching off.

#### **Personal information**

Fact: 12% of 10 to 14 year olds share personal information online<sup>2</sup>

- **1.** Get your child on side with online privacy by exploring how their personal information can be used now and in the future.
- 2. If you have your own social media account, think about the types of photos and information you share. Do you post photos of your child that show details of their school, sporting club or other activities? Take the opportunity to review your own habits and model safe online behaviour.
- Get involved—play along with your child to get a feel for how they are managing their online privacy in the gaming world.

active social media accounts

23<sub>hrs</sub> per week



share personal information online

'2016 Parental Information Needs and Digital Youth Participation Survey – A nationally representative sample of 2278 children and youth (8-17 years)

<sup>3</sup>2017 Youth Digital Participation Survey – A nationally representative sample of 3017 children and youth (8 – 17 years). Personal information includes sharing full name, birthday home address, home phone number, mobile phone number, email address, something that shows their face, something that shows their school.

ame of their school.

Source: https://esafety.gov.au/iparent



### Inappropriate content (the nasty stuff! – like violence, offensive or sexually explicit material)

Fact: 9% of 10 to 14 year olds reported being exposed to inappropriate content<sup>3</sup>

- Be vigilant, especially if your child is prone to taking risks or is emotionally or psychologically vulnerable.
- 2. You can use parental controls, filtering software and safe searches (like Google Safe Search) to help block some of the nasty stuff. Remind your child not to open spam email or click on pop-ups.
- 3. Keep your child connected to trusted friends and family online and offline and discuss the importance of healthy and respectful relationships.

#### Cyberbullying

Fact: 21% of 10 to 14 year olds reported being socially excluded by others online (one form of cyberbullying)<sup>3</sup>

- 1. Young people might not tell their parents about cyberbullying. They may be embarrassed or worried you might overreact, restrict access to devices or make things worse if they speak out. Try to respond calmly. Listen first, then act.
- 2. Be aware—key signs can include being upset after using devices, changes in personality, a decline in school work and appearing lonely and distressed.
- **3.** Report serious cyberbullying material to the social media service where it happened. You can also <u>submit a complaint to us</u> if the reported material has not been taken down within 48 hours.

#### **Contact with strangers**

Fact: 36% of 10 to 14 year olds said they had talked to strangers online<sup>3</sup>

- 1. Help your child understand why it's important to be vigilant about new online 'friends'. Someone who says they are a 12-year-old girl or boy could actually be a 40-year-old man!
- 2. Encourage your child to tell you or another trusted adult if they feel uncomfortable or worried about online contact with a stranger—there are tools in social media and in online gaming that can help block people.
- 3. Work with your child to save examples of the messages in case you want to follow up with the police. Taking screenshots is easy, use the print screen (PrtScrn) button on your computer or the Shift-Command-4 function on a Mac. You can also use your phone to take a quick photo of their device with the message.





36% talked to strangers online

<sup>3</sup>2017 Youth Digital Participation Survey – A nationally representative sample of 3017 children and youth (8 – 17 years).

Source: https://esafety.gov.au/iparent



This sheet is a resource that will help you to have a structured conversation with your children about difficult topics. It includes example sentences and answers which can help you navigate a conversation about digital security and privacy with your child. The following discussion points are important and often difficult topics to broach. Each discussion point below may be useful for your child and yourself in discussing cyber-security and an opportunity to do further online research together.



Write a list of the sites and apps you each use on a regular basis. If there are any sites you aren't familiar with, ask:

- "Who uses the app/site?" (E.g. Teenagers, business people, people of all different ages, etc.).
- "Why do they use the app/site?" (E.g. To connect with friends, to stay up-to-date, to plan events, etc.).
- "Where can they change the privacy settings on the app/site?" (E.g. How they can control who can see information about them on the app/site?).



Be careful about posting the following on social media:

- Birth dates
- Addresses
- Information about your daily routine
- Holiday plans
- Where you go to school or work
- Photos of you or your family and friends



Talk about what could happen if their accounts were compromised by asking the following questions:

- "What information might you lose if someone gained access to your account?" (E.g. Your photos, your messages, your videos, etc.).
- "What information on this site/app would you not want other people to know about?" (E.g. Your address, your phone number, your personal photos, etc.).
- What should you do so this doesn't happen again?





Discuss the importance of having a strong password:

- Use a combination of words that you can remember, but which aren't obvious. For example, the passphrase "diversity labyrinth sighed soprano almost died" is the same as a 46-character password (most websites only require 6 characters), but much easier to remember.
- Make sure your combination doesn't contain personal information (E.g. Names, birthdays, etc.) that can be found out through social media or other means.
- Avoid popular culture phrases (i.e. Music, movies, TV shows, etc.) as inspiration for your password.
- Get a rough idea of how strong your password is by visiting the website https://howsecureismypassword.net/



Make sure your phone is secure (i.e. activate PIN security, fingerprint passwords, etc.).



Discuss which sites/apps know your location and how do you make sure this information isn't shared with others.



f your child ever sees or receives anything online that makes them uncomfortable, they should discuss it with you, friends or teachers. Alternatively, they can call the Kids Helpline at 1800 55 1800 or go to https://www. yourtown.com.au/apps/webcounselling/live/chat/



If you are unsure about any of the information contained in this document or want to know more, check the resources section of the Optus Digital Thumbprint website: http://www.digitalthumbprint.com.au/resources/



If you or your child wanted to report cyberbullying, you can go to https://esafety.gov.au/complaints-andreporting/cyberbullying-complaints/i-want-to-reportcyberbullying/



Make sure they have the strongest privacy settings on all social media sites so that only close friends can view their information, tag them in photos or share posts. The website <a href="https://www.esafety.gov.au/esafety-">https://www.esafety.gov.au/esafety-</a> information/games-apps-and-social-networking has a guide to the security and privacy settings of many popular sites and applications.



The legal age to have an account on most social media sites (including Facebook, Twitter and Instagram) is 13. If you are unsure of the age restrictions, make sure to check the site's terms and conditions.



Be wary of giving information to people you don't know.



This sheet is intended to help you have a discussion with your child about how to study in the most effective way. Below, we have a number of useful study applications and suggested questions that you and your child can ask each other about how you both learn to do new things and manage your time. By sharing your experiences with your child, we hope that you both improve your productivity in both study and work. Each question should be answered by your child AND yourself.

## Applications that help you create flashcards/quizzes and study schedules

Research has shown that retrieval practice is one of the most effective ways of studying. Retrieval practice is testing yourself regularly about the key ideas in anything new you're learning. One common way of this is creating flashcards on the key ideas as you're reading the material for the first time and then testing yourself as a way of studying the material.

Research also shows that if you spread out what you are studying so that you revise material just before you're about to forget it, your long-term learning will be much better.

These free programs allow you to create your own flashcards or quizzes and then use an algorithm to estimate when it's best to show the flashcards or quizzes for long-term learning.

- Anki <a href="http://ankisrs.net">http://ankisrs.net</a>
- Cobocards <a href="http://www.cobocards.com">http://www.cobocards.com</a>
- Brainscape https://brainscape.com
- Memrise <a href="https://www.memrise.com">https://www.memrise.com</a>
- Mnemosyn <a href="http://www.mnemosyne-proj.org">http://www.mnemosyne-proj.org</a>
- Supermemo http://supermemo.com
- Synap <a href="https://synap.ac">https://synap.ac</a>

### Applications that reduce/block distractions

One of the biggest problems for modern students is the number of online and mobile distractions that hinder effective study.

Many of these websites and programs have hundreds of engineers designing them to figure out the best way to get people to use them and keep using them, so it's not a surprise that many students give into the temptation to check their phone or surf the web for a minute and then find out that they've wasted most of their study time.

#### Rescuetime:

 This program shows you how you're using your time and gives you detailed reports and data based on your computer activity. It doesn't work on iPhones. https://www.rescuetime.com

#### Toggl:

 This program gives you an overview of how much time you have spent on different tasks. https://www.toggl.com

#### Freedom:

 This program enables you to block websites and apps based on "blocklists" that you create. You can set them for any time and place. https://freedom.to

#### Leechblock (Firefox) and StayFocusd (Chrome):

 These browser ad-ons organise websites into categories and lets you set how and when to block them.

#### Applications to help you organise yourself

#### Todoist:

This program allows you to manage what you need to do. https://todoist.com

#### Evernote:

This program is designed for note-taking, organising and archiving. https://evernote.com

#### Pomodoro Timer:

The Pomodoro technique is a technique where you focus for 25 minutes, then take a 5-minute break, and then continue focusing for another 25 minutes. Using this technique enables you to avoid multi-tasking and concentrate for 25 minutes before taking a break.

https://gigaom.com/2010/11/10/9-free-pomodoro-timers

If you are unsure about any of the information contained in this document or want to know more, check out the resources section of the Optus Digital Thumbprint website: http://www.digitalthumbprint.com.au/resources

#### Questions about managing your time

- 1. How do you learn to do new things at work/school?
- What is the biggest reason you're not productive at work/school?
- 3. When do you think you're most productive? Is there anything different in that situation that you can use to improve your productivity at other times?
- 4. How do you think technology helps your productivity at work/school? How do you think technology hurts your productivity at work/school?
- 5. Are there any "productivity hacks" from work/school that you can learn from each other?
- 6. How do you manage your time at work/school?



This sheet is intended to help you have a discussion with your child about cyberbullying and online interaction. Below, we have suggested topics you can discuss with your child. The following discussion points are important and often difficult topics to broach. The intention is to show both bullying and its solutions can happen in the school environment and the adult world. Each topic below should be discussed by both your child AND yourself.



Talk about bullying that you have seen at your school/ your workplace (past or present).





Both describe what you think an inappropriate picture is. Are there any differences?



How could you respond if someone you knew (at school/work) was being bullied?

(e.g. Report bullying if you see it, offer your support for those who are being bullied, etc.)



Take one post or comment from both of you on social media. Compare the two. Ask if they would post the same messages to a teacher, parent or someone they knew well. Would they say the same thing if they were face to face with someone? Why/Why not?



Why might someone post pictures of themselves (school-age/adult)?

(i.e. To please friends or partners, to get approval from friends and strangers, to make friends and strangers jealous of their lifestyle, to share what is happening in their life with friends, etc.)



What do you (student) think could go wrong if someone asked you to send a provocative picture? What are your options? Can you prevent or minimise what could go wrong?

(e.g. It might get passed on to people it was not intended for (friends, parents, teachers and strangers), there might be legal implications, you could choose not to send the picture, or discuss some rules with your partner, etc.)



What would you do to help someone who is being bullied at school/work?

(e.g. Report it, talk to the person being bullied, talk to the bully, etc.)  $\,$ 



What would you do if someone was cyberbullying you (at school/work)?

(If possible, bring up how bullying is handled at your workplace (with reference to the HR department) to show that there are often official processes and procedures to handle bullying.)



What do you (student and parent) think you can do to be a better digital citizen?

(e.g. Report bullying if you see it, offer your support for those who are being bullied, think about how other people might feel about the comments you make, think about what might happen if your comment went viral, etc.)



If you are unsure about any of the information contained in this document or want to know more, check the resources section of the Optus Digital Thumbprint website: http://www.digitalthumbprint.com.au/resources/

### **OPTUS PARTNERSHIPS**

## Optus Digital Thumbprint



If you need more help or information contact Kids Helpline.

*2* 1800 55 1800

kidshelpline.com.au



Office of the eSafety Commissioner

For more resources and information, visit the Office of the eSafety Commissioner website.

esafety.gov.au



If you also have younger children, DQ World is designed for ages 8 - 12 and teaches 8 digital citizenship skills.

dqworld.net



### The smart way for families to manage content and time online, on any device



#### TIME LIMITS

Limit daily screen time for platforms, apps, and more.



Disable access to the Internet for users or the entire home.



Set individual filter levels for each family member.



#### BEDTIME

Make late night surfing a thing of the past with BedTime.



#### OFFTIME

Set "no Internet" times during the day.



#### **REWARDS**

Give extra Time Limits or a later BedTime for the day.



#### **USAGE**

Compare time online today, last week, or even last month.



Block ads, enable Safe Search, and manage guest devices.



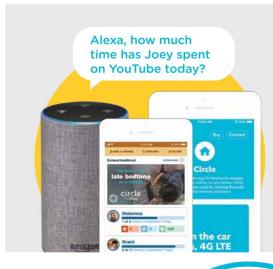
Cyber Available now at SafeHouse cybersafehouse.com



# circle go

Your family's mobile devices, now managed across all networks.

Circle Go takes all of the settings your kids' devices have at home and extends them to 4G LTE and any other Wi-Fi network they join.



## circle connections

Circle Connections enable your family to connect your favorite devices, apps, and services to do things like reward screen time for chores and ask Alexa questions about your Circle.











"Circle has changed our lives. No more taking away electronics and fighting over screen time. Love it."

Renee H.

"Circle with Disney has become my favorite Digital Parenting tool! It's an all-in-one solution to help manage all-in-one devices. I recommend it daily in my clinical office and in my digital parenting workshops."

Dr. Adam Pletter, Psy.D.

"Love Circle! Saved our internet issues with three teens, and a seven year old. Bedtimes are actually happening again! And I love that I can Pause the Internet for one child while leaving others unaffected."

Joanne H.





\$39.00 Off with Discount Code:

SBC2018



iPhone 7 Plus

iPhone 6s Plus

iPhone 6 Plus

iPhone 6s

iPhone 6

iPhone SE

iPhone 5s

# 2018 Cyber Awareness Evening

### Using App Limits and Downtime in IOS 12



#### iOS 12 is compatible with these devices. iPhone iPod iPad iPhone Xs 12.9-inch iPad Pro iPod touch (6th (2nd generation) iPhone Xs Max generation) iPhone XR 12.9-inch iPad Pro iPhone X (1st generation) iPhone 8 10.5-inch iPad Pro iPhone 8 Plus 9.7-inch iPad Pro iPhone 7 iPad (6th

generation)

generation)

iPad (5th

iPad Air 2

iPad mini 4 iPad mini 3

iPad mini 2

iPad Air



### **Accessing Screen Time**

- 1. Open up the settings app.
- 2. Scroll down to the "Screen Time" section that's grouped with Notifications, Sounds, and Do Not Disturb.
- 3. Tap on "Screen Time" to see your usage statistics.



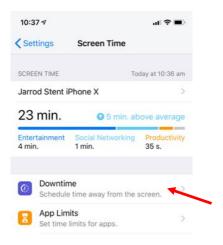


### Restrictions with Screen Time

#### Downtime:

Much like setting up Bedtime Mode in Do Not Disturb, users can set a scheduled time at which the device effectively shuts down for a specific length of time, allowing access only to calls and apps you allow. You simply choose a start time and an end time, which is useful if you want to restrict your child's access at bedtime or during family time.

- 1. In the Screen Time settings, choose "Downtime".
- 2. Toggle "Downtime" on.
- 3. Choose a start time and an end time.





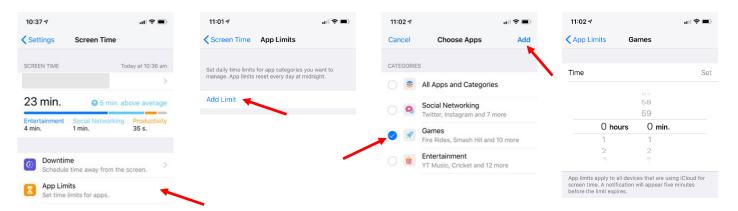




#### App Limits:

App Limits lets you restrict access to a specific category of apps for a set period of time per day. For example, if the games category is restricted to 30 minutes, after 30 minutes of game play, whether it be one app or multiple game apps, any app in the game category will not be available.

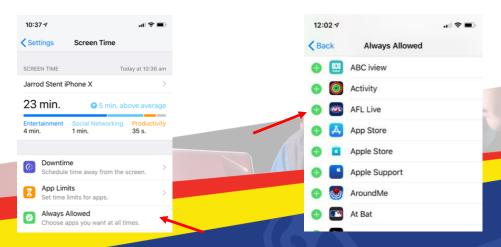
- 1. In the Screen Time settings, choose "App Limits".
- 2. Choose "Add Limits".
- Choose an App Category to limit. You can select multiple categories or select all.
- Add a time limit.



#### Always Allowed:

"Always allowed" works in conjunction with downtime. By Default, Phone, Messages, FaceTime and Apple Maps are enabled. Add apps to enable access when Downtime is in use.

- 1. In the Screen Time settings, choose Always Allowed.
- 2. Select the green plus sign next to an app to allow use of it during "Downtime".

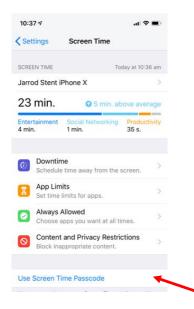




## Set a passcode for Screen Time

The passcode can be used to secure Screen Time settings as well as securing "App Limits". By default, when an app limit has been reached, a warning will display on the screen indicating that the time limit is up. The user can then ignore or extend the limit. With a passcode set, the user cannot ignore or extend a limit.

- 1. In the Screen Time settings, select "Use Screen Time Passcode"
- 2. Enter a 4-digit code. You will have to enter this code again as verification.







### St. Bede's College Acceptable Use of ICT Agreement

The Acceptable Use ICT Agreement contains six principles for being a responsible Digital Citizen.

#### These are:

Respect Yourself. I will show respect for myself through my actions. I will select online names that are appropriate, I will consider the information and images that I post online. I will only post content to my online entries which shows myself, my peers, the school and the wider community in the best light and perspective. I will consider what personal information about my life, experiences, experimentation or relationships I post. I will not be obscene.

**Protect Yourself.** I understand that all material published is not private and is subject to view by a wide range of people including members of the school as well as the wider community. I will ensure that the information, images and materials I post online will not put me at risk. I will not publish my personal details, contact details or a schedule of my activities. I will report any attacks or inappropriate behaviour directed at me. I will protect passwords, accounts and resources.

Respect Others. I will show respect to others. I will not use electronic mediums to flame, bully (cyberbully), harass or stalk other people. I will show respect for other people in my choice of websites, I will not visit sites that are degrading, pornographic, racist or inappropriate. I will not abuse my rights of

access and I will not enter other people's private spaces or areas. I will use the facilities for the purpose they were intended, my emails, posts, comments and content will have an educational focus.

**Protect Others**. I will always report abuse or inappropriate behaviour to safe guard my safety and the safety of my peers and community. I will not forward inappropriate materials or communications; and not visit sites that are degrading, pornographic, racist or inappropriate.

**Respect Intellectual property**. I will request permission to use resources. I will suitably cite any and all use of websites, books, media etc. I will validate information. I will use and abide by the fair use rules.

**Protect Intellectual Property.** I will request to use the software and media others produce. I will use free and open source alternatives rather than pirating software. I will purchase, license and register all software. I will purchase my music and media, and refrain from distributing these in a manner that violates their licenses. I will act with integrity.

I will, in all matters online, conduct myself in a moral and ethical manner

It is expected that all members of the College community will abide by these guiding principles in their use of any form of electronic facilities.

### Extract from the St Bede's College ICT Device Agreement

The following is taken from the St Bede's College ICT Device agreement that was signed by students and parents:

#### The student is responsible for:

- 2.1. Bringing the device **fully charged** to school every day. Devices cannot be charged at school.
- 2.2. Taking the device to every class unless instructed otherwise by a teacher.
- 2.3. Adhering to the St Bede's College Acceptable Use of ICT Agreement which is attached and available on the College Intranet.
- 2.4. Backing up data securely on Google Drive and at home.
- 2.5. Ensuring the identification stickers/labels are not removed from the device or bag. This may void warranty.
- 2.6. Keeping the device secure when not in use at school by placing it in their locker that has a school issued combination lock.
- 2.7. Ensuring that settings for virus protection that has been installed are not disabled or removed.
- 2.8. Ensuring the device is not physically altered or modified in any way without the express permission of the Deputy Principal for ICT and Infrastructure. No software installed on the device should be altered or removed unless directed by the College. The modification of operating system software is not permitted.
- 2.9. St Bede's College reserves the right to inspect any student device if there is a reason to believe school policies have been violated. St Bede's College may monitor use of ICT resources (including all network traffic, email, etc.) to ensure compliance with school policies. Students agree not to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.

Following appropriate safety and care procedures such as:

- Transporting the device in the case provided at all times.
- · Handling the device carefully and taking care not to drop it.
- Ensuring that food and drinks are kept well away from the device.
- Ensuring that no items e.g. earphones are left lying on the screen before closing the cover.

# The 12 Protocols for using my ICT Device responsibly for learning.

These protocols are based on the St Bede's ICT Acceptable Use Agreement ICT Device Agreement and should be read in conjunction with those documents.

The term ICT device refers to iPads, Notebooks, Netbooks, Mobile Phones, and similar devices.

- I will bring my ICT Device to school fully charged each school day. I will protect my device to the best of my ability including using any protective covers provided. I will protect my school bag against damage when it contains my ICT device. I will not use my device when travelling to or waiting outside classrooms.
- 2. I will ensure that my home screens or desktop contains only school approved apps and links, with appropriate wallpaper and language. I will use a passcode or password to protect against unauthorised use by others.
- I will only open my ICT Device and use applications and websites when directly instructed to do so by my teacher.
   I will not use personal content during class time unless directly linked to my learning and with prior knowledge of the classroom teacher.
- 4. All apps/programs in my multitasking bar or taskbar will be closed at the beginning of each lesson unless they are directly related to my studies.
- When not using my ICT Device in class, the lid or smart cover will remain closed at all times opening of the lid or smart cover will only occur after teacher instructions to do so. When the teacher instructs the lid or smart cover to be closed I will do so immediately.
- 6. During class time, I will not use my ICT Device for playing games. All devices will remain on mute unless the teacher requests otherwise.
- 7. I will only take and use photographs, recordings and videos of other students or staff with their express prior permission and knowledge and only in relation to school work. I will not use or distribute any such images for any other purpose, be it by soft or hard copy.
- 8. I will ensure that all personal content is appropriate at all times and I will leave sufficient memory for school related content. Any use of technology to obtain unauthorised access to other devices or cause disruption on the computer network is strictly not permitted.
- 9. When on school property, I will only access the internet through the College WiFi system. I will not tether my iPad or Notebook to another device whilst at school. I am aware in relation to the use of my device, the Internet and e-mail, Section 474.17 of the Criminal Code Act states that a person is guilty of an offence if they knowingly or recklessly:
  - Use a telecommunications device supplied by a carrier in such a way as would be regarded by reasonable persons as being, in all circumstances, menacing, harassing or offensive.
- 10. I will not attempt to contact or friend teachers through social networking sites. I will not comment on teachers in a derogatory way on any website.
- 11. When emailing or contacting teachers directly I recognise that teachers will only respond in a timeframe which is reasonable and usually during working hours.
- 12. I will ensure that I am fully aware of, fully understanding of and compliant with these Protocols and with the ICT Acceptable Use Agreement Cybersafety guidelines as available on the College intranet. I am aware these may change.

If I am not responsible in my use of the iPad or Notebook and breach the above, then I understand that appropriate disciplinary actions may be taken which may include the confiscation of my ICT device.