Student Cyber Safety and Acceptable Computer Use Policy

This document is comprised of two sections:

Section A – Cyber safety in the College Environment
(I) Important Sunshine College cyber safety initiatives
(II) General cyber safety rules
Section B – Information Specifically for Sunshine College Students
(I) Additional information
(II) Additional rules / responsibilities

Instructions for students:
1. You and your parent/legal guardian/caregiver are asked to read Section A 'Cyber Safety in the College Environment' and Section B
'Information Specifically for Sunshine College Students' carefully.

2. If help is needed to understand all the language, or there are any points your family would like to discuss with the College, let your Campus Principal know.

3. The student and their parent/legal guardian/caregiver need to sign the Student Notebook User Agreement.

4. It is important to be aware that changes to these Guidelines and the Student Notebook User Agreement can occur without notice and will be posted on the College's website at www.sunshine.vic.edu.au

Section A – Cyber safety in the College Environment

SECTION A (I) IMPORTANT SUNSHINE COLLEGE CYBERSAFETY INITIATIVES
The values promoted by Sunshine College include: Growth, Learning, Relationships, and Wellbeing. Sunshine College is an eSmart school. The cyber safety of the College environment which Is outlined in this document and are based on these core values.

The College's computer network, Internet access facilities, computers and other College ICT equipment/devices, such as student Notebooks, bring great benefits to the teaching and learning programs at Sunshine College, and to the effective operation of the College. However, it is essential that the College endeavours to ensure the safe use of ICT within the College community.

Sunshine College has rigorous cyber safety expectation for its learning community.

The cyber safety education supplied by the College to its learning community is designed to complement and support the safe use of ICT. The overall goal of the College in this matter is to create and maintain a cyber-safe College.

Requirements regarding appropriate use of ICT in the College learning environment

In order to meet the College's legislative obligation to maintain a safe physical and emotional learning environment, and be consistent with the values of the College:

- The use of **the College's** computer network, Internet access facilities, computers and other College ICT equipment/devices, including but not limited to iPads, and student Notebooks, on *or* off the College site, is limited to educational purposes appropriate to the College environment. This applies whether or not the ICT equipment is owned by the user or is owned/leased either partially or wholly by the College. If any other use is permitted, the user(s) will be informed by the College.

- The College has the right to monitor, access, and review all the usage undertaken.

- The College will use remote access software to ensure appropriate use of ICT devices and the College network. This includes personal emails sent and received on the College's computers and/or network facilities, either during or outside College hours.

The use of any **privately-owned/leased** ICT equipment/devices on the College site, or at any College-related activity must be appropriate to the College environment. This includes any images or material present/stored on privately-owned/leased ICT equipment/devices brought onto the College site, or to any College-related activity.

Such equipment/devices could include a Notebook, desktop, iPad, mobile phone, camera, recording device, or portable storage device (like a USB or flash memory device). Anyone unsure about whether or not it is appropriate to have a particular device at College or at a College-related activity, or unsure about whether the planned use of a particular device is appropriate, should check with the campus principal.

Note that examples of a **'College-related activity'** include, but are not limited to, a field trip, camp, sporting or cultural event, *wherever its location*.

When using a global information system such as the Internet, it may not always be possible for the College to filter or screen all material. This may include material which is **inappropriate** in the College environment (such as 'legal' pornography), **dangerous** (such as sites for the sale of weapons), or **illegal**.

However, the expectation is that each individual will make responsible use of such systems. In the event of their use, students must be able to demonstrate their connection to current classroom learning.

Monitoring by the College

Sunshine College has an electronic access monitoring system which has the capability to record Internet use, including the user details, time, date, sites visited and from which computer or device the http traffic was viewed. The College also has the ability to remotely monitor College ICT equipment, via logs and real-time screen viewing, including student Notebooks and iPads. You must not attempt to prevent/ block the College representatives from remotely monitoring any ICT equipment/device.

The College monitors traffic and material sent and received using the College's ICT infrastructures. This will be examined and analysed to help maintain a cyber-safe College environment.

The College will deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email.

The College holds the right to access/redirect/stop/copy for evidence of any type of electronic data and remove inappropriate electronic data without notice.

The College holds the right to lock/disable/remove/modify domain/local computer accounts in the event of a threat to the College ICT systems. This includes any electronic devices which are on the premises of the College.

It is the expectation that each individual will be responsible in their use of ICT.

Ownership
Notebooks, desk tops and iPads remain the property of the College.

The College reserves the right to confiscate any Notebooks /Ipad / ICT equipment due to breaches to these guidelines.

Audits
The College will from time to time conduct an internal audit of its computer network, Internet access facilities, computers and other College ICT equipment/devices, or may commission an independent audit. If deemed necessary, auditing of the College computer system will include any stored content, and all aspects of its use, including email. An audit may also include any Notebooks, Desk tops or iPads provided or subsidised by/through the College or subsidised by a College-related source such as the Department of Education and Training.

Breaches of these guidelines and the Student Notebook User Agreement
Breaches to guidelines and the agreement can undermine the values of the College and the safety of the learning environment, especially when ICT is used to facilitate misconduct.

Such a breach which is deemed harmful to the safety of the College such as involvement with inappropriate or illegal material, anti-social activities such as *harassment and bullying* and possession of Peer-to-Peer software such as Limewire or BitTorrent will constitute a significant breach of discipline and result in serious consequences. A breach will result in the Notebook or ICT device being reimaged. Any further breaches of this nature will result in changes to the management of the Notebook or ICT device. A college representative will respond and take appropriate action regarding consequences of all breaches.

If there is a suspected breach involving privately-owned ICT on the College site or at a College-related activity, the matter may be investigated by the College. The College may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.

Involvement with **material** which is deemed 'age-restricted', or 'objectionable' (illegal) is a very serious matter, as is involvement in an **activity** which might constitute criminal misconduct, such as harassment. In such situations, it may be necessary to involve law enforcement, including federal police and agencies; in addition to any disciplinary response made by the College as a result of its investigation.

Other aspects of the College's cyber safety programme
Other cyber-safety initiatives, such as cyber-safety education supplied to the College community can be found by browsing the web. This education plays a significant role in the College's overall cyber-safety programme, and also helps keep children, young people and adults cyber-safe in all areas of their lives. If more information is required, please contact the College. Two sites on cyber safety can be found at the following links:

www.bullyingnoway.gov.au

www.cybersmart.gov.au

SECTION A (II) - GENERAL CYBERSAFETY RULES

These general rules have been developed to support the Sunshine College Cyber - Safety Initiative's outlined earlier.

Use of any ICT must be appropriate to the College environment and for educational purposes only. The College's computer network, Internet access facilities, computers and other College ICT equipment/devices is to be used only for educational purposes.

This rule applies to use on *or* off the College site. If any other use is permitted, the College will inform the user/s concerned.

Any student who has a signed an agreement with the College and allows another person who has not signed a College user agreement, to use College ICT equipment and systems is responsible and liable for that use.

Use of privately-owned/leased ICT equipment/devices on the College site, or at any College-related activity must be appropriate to the College environment. This includes any images or material present/stored on privately-owned/leased ICT equipment/devices brought onto the College site or to any College related activity.

It also includes the use of mobile phones. Any queries should be discussed with the campus principal.

When using College ICT, or privately-owned ICT on the College site or at any College-related activity, users must not:

- initiate access to inappropriate or illegal material – including but not limited to adult content, online gaming sites, gambling sites, social networking sites such as Facebook. The use of Peer-to-Peer software is also prohibited.
- save or distribute such material by copying, storing or printing.

In the event of accidental access of such material, users should:

1. not show others
2. close or minimise the window
3. report the incident
    - Students should report to a teacher immediately
    - Staff should report such access as soon as practicable to the campus administration.

Under no circumstances should ICT be used to facilitate behaviour which is either inappropriate in the College environment or illegal. Cyber Bullying will not be tolerated.

Individual user name and password. If access is required to the College computer network, computers and Internet access using College facilities, it is necessary to obtain a personal user account from the College.

Confidentiality of passwords. It is important to keep passwords confidential and not shared with anyone else.

Access by another person. Users should not allow another person access to any equipment/device login under their own user account, unless with special permission from an assistant principal or campus principal. (Any inappropriate or illegal use of the Sunshine College computer facilities and other College ICT equipment/devices may be traced by means of this login information.)

Appropriate use of email. Those provided with individual, class or group e-mail accounts are expected to use them in a responsible manner and in accordance with the Student Notebook User Agreement. This includes ensuring that no electronic communication could cause offence to others or harass or harm them, put the owner of the user account at potential risk, or in any other way be inappropriate in the College environment.

Disclosure of personal details
For personal safety, users should be very careful about revealing personal information about themselves, such as home or email addresses, or any phone numbers including mobile numbers. Nor should such information be passed on about others.

Care of ICT equipment/devices
All College ICT equipment/devices should be cared for in a responsible manner and especially ensuring that Notebooks and iPads are carried in the bags or cases if provided.
Any damage, loss or theft must be reported immediately to the campus principal. In the event of theft, a police statement must be made as soon as practically possible.

At school, when Notebooks or iPads are not being used or carried by the individual they should be securely stored in a locked locker.

Notebook/ICT devices must be returned to the College in the same condition as was initially supplied. That is, no stickers, graffiti, white-out, scathes and etchings, cracks, missing keys, discolouration, substances requiring more than light cleaning or any damage beyond normal wear and tear.

All users are expected to practice sensible use to limit wastage of computer resources or bandwidth. This includes unnecessary Internet access, uploads or downloads.

Connecting software/hardware
Users must not attempt to download, install or connect any unauthorised software or hardware onto College ICT equipment, including but not limited to student Notebooks and iPads or utilize such software/hardware. Any user with a query or a concern about this issue should speak to the campus principal.

In a special case where permission has been given by the campus principal or delegate to connect or install privately-owned equipment/devices or software, it is with the understanding that the College may scan this equipment/device/software at any time thereafter as part of a regular or targeted security check, such as for viruses.

Copyright and licensing
Copyright laws and licensing agreements must be respected. This means no involvement in activities such as illegally copying material in any format, copying software, downloading copyrighted video or audio files, using material accessed on the Internet in order to plagiarise, or illegally using unlicensed products. This means that students are not to have limewire or torrents or any other peer to peer software on the Notebooks / ICT device. If students are found in breach of these guidelines the Notebook / ICT device will be reimaged immediately.

The College will provide software which is in accordance with the copyright laws and must only be installed on College leased or owned equipment. Once equipment ownership transfers outside of the College it is only legal to have installed the software which originally came with the computer and copyright laws and licensing agreements become the responsibility of the equipment holder.

Posting material
All material submitted for publication on the College Internet/Intranet should be appropriate to the College environment.

Such material can be posted only by those given the authority to do so by the campus principal or their delegate. The college ICT technicians should be consulted regarding links to appropriate websites being placed on the College Internet/Intranet (or browser homepages) to provide quick access to particular sites.

Queries or concerns
Staff and students should take any queries or concerns regarding technical matters to the campus principal or their delegate.

Queries or concerns regarding other cyber-safety issues should be taken to the campus principal. In the event of a serious incident which occurs when the campus principal is not available, another member of Principal Class Team should be notified immediately.

Section B – Information Specifically for Sunshine College Students

SECTION B (I) Additional information

While at College or a College-related activity, you must not have involvement with any material or activity which might put yourself at risk. The use of social networking sites, including but not limited to Facebook are therefore prohibited. As well, you must not at any time use ICT to upset, harass, or harm anyone else in the College community, or the College itself, even if it is meant as a 'joke'. Unacceptable use could include acts of a malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, gaming, impersonation/identity theft, spoofing, gambling, fraud, copyright infringement, or cheating in an examination. Inappropriate behaviour the College may need to respond to also includes the use of websites to facilitate misconduct which puts at risk the safety of the College environment.

If any privately-owned ICT equipment/device, such as a Notebook, desktop, PDA, mobile phone, camera, or recording device, portable storage (like a USB or flash memory device), is brought to College or a College-related activity, the College cyber-safety rules apply to that device. **If you are not sure whether it is appropriate to have a particular device at College or at a College-related activity, you are expected to check with the relevant teacher before bringing it.**

Monitoring

The College reserves the right at any time to check work or data on the College's computer network, Internet access facilities, computers and other College ICT equipment/devices. For example, in order to help make sure that the College stays cyber-safe, teachers may at any time check student email or work. The eLearning Team members also have the ability to remotely monitor College ICT equipment, via logs and real-time screen viewing, including student Notebooks and iPads. You must not attempt to prevent the ICT Management Team from remotely monitoring any ICT equipment/device.

If there is a suspected breach of use agreement involving privately-owned ICT, the matter may be investigated by the College. The College may ask to check or audit that ICT equipment/device as part of its investigation into the alleged incident.

Consequences.

Depending on the seriousness of a particular breach, an appropriate response will be made by the College. Possible responses could include one or more of the following: a discussion with the student, informing parents/legal guardian/caregiver, reimaging of Notebook/device, loss of administrator access to Notebooks/devices, loss of student access to College ICT, taking disciplinary action. If illegal material or activities are involved, it may be necessary for the College to inform the police and/or other government departments.

Where Notebooks require reimaging due to a breach of this agreement, the Notebook/ICT device will not be backed up before reimaging. There will be no opportunity given to the student to back up their work.

The College reserves the right to confiscate the Notebook or iPad due to a breach in the expectations listed in the Student Notebook User Agreement.

SECTION B (II) - ADDITIONAL RULES / RESPONSIBILITIES

Accessing the Internet at College on College ICT. The only time you can access the internet at the College or on a College computer of any kind during class is when a teacher gives permission and there is staff supervision. While at school, students are only to use the school student internet connection. Students are not to connect to any external devices e.g. Phones, USB modems or other wireless networks while at Sunshine College. Students found breaching these guidelines will lose access to Sunshine College's network, and Notebooks will be reimaged immediately. Deliberate circumvention of school internet filtering, by use of third-party software, external internet connections (such as '3 mobile internet'), or "anonymous proxy" sites will result in the Notebook / ICT device being immediately reimaged, the administrator status of the student will be modified and the student's ability to access the Sunshine College network will be reviewed.

Borrowing College ICT.
If you have permission to use College ICT equipment at home or anywhere else away from College, it must not be given to anyone else to use unless at the direction of a staff member. The College ICT is to be used only for the purpose it was lent, and you should explain this to your family or whoever else you are with. If a problem occurs, you must report it to the relevant teacher straight away. *You are responsible as you have signed the Notebook User Agreement.*

Mobile phones.
Cyber-safety rules also apply to mobile phones. Students must not use mobile phones for involvement with inappropriate material
or activities, such as:
• upsetting or harassing students, staff and other members of the College community even as a 'joke'.
• inappropriately using text, MMS, email, photographs or film, phone messages, web browsing, images or any other functions.
• during any assessment where such possession or use is specifically prohibited.

Care of the computers and other College ICT equipment/devices, and their appropriate use includes:
You must not damage or steal any equipment, or try to damage the ICT network. If the damage is deliberate, it will be necessary for the College to inform your parent/legal guardian/caregiver who will have responsibility for the cost of repairs or replacement.

Students need permission from staff to:
• print material when in the classroom situation. Any material printed out of class must be appropriate in the College environment.
• contribute material to the College Internet/Intranet site. As well, there should be no student involvement in any unofficial College Internet/Intranet site which purports to be representative of the College or of official College opinion.
• send email to groups of users which are available on college e-mail/exchange server(s). Only email to individual students and staff according to the e-mail agreements are to be sent.

Students must be considerate of other users. This includes:
• sharing with other users and not monopolising equipment.
• avoiding deliberate wastage of ICT-related resources including bandwidth, through actions such as unnecessary printing, and unnecessary Internet access, uploads or downloads.
• no intentional disruption of the smooth running of any computer or the College network.
• avoiding involvement in any incident in which ICT is used to send or display messages/communications which might cause offence to others. Examples include text messaging, email messages, or creating, displaying or sending inappropriate graphics, and recording or playing inappropriate audio or video files.
• obtaining permission from any individual before photographing, videoing or recording them.

Respect for privacy, safety and security when using the Internet and ICT includes:
• if you accidentally access inappropriate, dangerous or illegal material you should:
1. not show others
2. close or minimise the window
3. report the incident to a teacher immediately.
• you should use data storage devices such as USB and flash memory devices, only in accordance with College regulations. This includes other portable devices such as USB hard drives.
• you must have no involvement in any activity which could put at risk the security of the College computer network or environment. For example, no involvement with malware such as viruses or involvement with any form of electronic vandalism or theft. This includes 'hacking' and any other physical or electronic activities that provide unauthorized access to the College ICT.