Onslow College Cybersafety Use Agreement

FOR ALL STUDENTS

FIRST NAME: _____

LAST NAME: _____

Initial Password: _____ (*5 characters or more, please keep a record)*

Year Level: _____

OFFICE USE ONLY

ID Number:

Student logon:

Form Teacher:

Dean:

To the student, and the parent/guardian/caregiver

1. Please read the entire document carefully, to check you understand your responsibilities under this agreement
2. Sign the appropriate section on this form
3. Complete and return this form to the school office
4. Check the **Cybersafety – Student Use Agreement** on our website for future reference and updates

We understand that Onslow College will:

- Do its best to keep the school cybersafe, by maintaining an effective cybersafety programme. This includes working to restrict access to inappropriate, harmful or illegal material on the Internet or school ICT equipment/devices at school or at school-related activities, and enforcing the cybersafety regulations and responsibilities detailed in use agreements
- Keep a copy of this signed use agreement form on file
- Respond appropriately to any breaches of the use agreements
- Provide members of the school community with cybersafety education designed to complement and support the use agreement initiative

Student's section

My responsibilities include:

- I will read the **Student Cybersafety at Onslow College** document carefully
- I will follow the cybersafety rules and instructions whenever I use the school's computer network, Internet access facilities, computers and other school ICT equipment/devices
- I will also follow the cybersafety rules whenever I am involved with privately-owned ICT devices/equipment on the school site or at any school-related activity, regardless of its location
- I will avoid any involvement with material or activities which could put at risk my own safety, or the privacy, safety or security of the school or other members of the school community
- I will take proper care of computers and other school ICT equipment/devices. I know that if I have been involved in the damage, loss or theft of ICT equipment/devices, my family may have responsibility for the cost of repairs or replacement
- I will ask the relevant staff member if I am not sure about anything to do with this agreement
- I give my permission for my picture and/or written work to appear in any official Onslow College publication including the school magazine, internet and intranet. No student's name will be published without their approval for that specific use

I have read and understand my responsibilities and agree to abide by this **Cybersafety – Student Use Agreement.** I know that if I breach this use agreement there may be serious consequences.

Signature: _____ Date: _____

Section for parental/legal guardian/caregiver

My responsibilities include:

- I have read the **Student Cybersafety at Onslow College** document carefully and discussed it with my son/daughter so we both have a clear understanding of my child's role in the school's effort to maintain a cybersafe environment
- I will ensure this use agreement is signed by my child and by me, and returned to the school
- I will encourage my son/daughter to follow the cybersafety rules and instructions
- I give my permission for my student's picture and /or written work to appear in any official Onslow College publication including the school magazine, internet and intranet. No student's name will be published without their approval for that specific use.

Parent/Legal Guardian/Caregiver (Please circle which term is applicable.)

Name: _____Signature: _____ Date: _____

STUDENT CYBERSAFETY AT ONSLOW COLLEGE

Section A – Cybersafety In The School Environment

- Important school cybersafety initiatives
- General cybersafety rules

Section B – Information Specifically For (Staff/Secondary Student)

- Additional information
- Additional rules/responsibilities
- Cybersafety Use Agreement Form

Important terms used in this document:

a. The abbreviation 'ICT' in this document refers to the term 'Information and Communication Technologies'.
b. 'Cybersafety' refers to the safe use of the Internet and ICT equipment/devices, including mobile devices.
c. 'School ICT' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below.
d. The term 'ICT equipment/devices' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 player), cameras (such as video, digital, webcams), all types of mobile phones, video and audio player/receivers (such as portable CD and DVD player), and any other, similar, technologies as they come into use.

SECTION A – CYBERSAFETY IN THE SCHOOL ENVIRONMENT

The school's computer network, Internet access facilities, computers and other school ICT equipment/devices bring great benefits to teaching and learning programmes at Onslow College, and to the effective operation of the school. (Examples of what is meant by 'ICT equipment/devices' can be found on page one.) However, it is essential that the school endeavours to ensure the safe use of ICT within the school community.

Thus Onslow College has rigorous cybesafety practices in place, which include cybersafety use agreements for all school staff and students.

1 Cybersafety use agreements

1.1 All staff and students, whether or not they make use of the school's computer network, Internet access facilities, computers and other ICT equipment/devices in the school environment, will be issued with a use agreement. They are required to read these pages carefully, and return the signed use agreement form to the school office.
1.2 Staff and students are asked to keep the other pages of the agreement for later reference. Updates will be made on the website.

2 Requirements regarding appropriate use of ICT in the school learning environment

In order to meet the school's legislative obligation to maintain a safe physical and emotional learning environment, and be consistent with the value of the school:
2.1 The use of the school's computer network, Internet access facilities, computer and other school ICT equipment/devices, on or off the school site, is limited to educational purpose appropriate to the school environment. This applies whether or not the ICT equipment is owned/leased either partial or wholly by the school. If any other use is permitted, the user(s) will be informed by the school.
2.2 The use of any privately-owned/leased ICT equipment/devices on the school site, or at any school-related activity must be appropriate to the school environment. This includes any images or material present/stored on privately- owned/leased ICT equipment brought onto the school site, or to any school-related activity.

Such equipment/devices could include a laptop, desktop, PDA, mobile phone, camera, recording device, or portable storage (like a USB or flash memory device). Anyone unsure about whether or not it is appropriate to have a particular device at school or at a school-related activity, or unsure about whether the planned use of a particular device is appropriate, should check with the Cybersafety Manager. Note that examples of a 'school-related activity' include, but are not limited to, a field trip, camp, sporting or cultural event, wherever its location.

2.3 When using a global information system such as the Internet, it may not always be possible for the school to filter or screen all material. This may include material which is inappropriate in the school environment (such as pornography), dangerous (such as sites for the sale of weapons), or illegal (which could include material defined in the Films, Videos and Publications Classification Act 1993, such as child pornography; or involvement with any fraudulent activity).

3 Monitoring by the school

3.1 Onslow College has an electronic access monitoring system which has the capability to record Internet use, including the user details, time, date, sites visited, length of time viewed, and from which computer or device.
3.2 The school monitors traffic and material sent and received using the school's ICT infrastructures. From time to time this may be examined and analysed to help maintain a cybersafe school environment.
3.3 The school will deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email.

4 Audits

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

5 Breaches of the use agreement

5.1 Breaches of the use agreement can undermine the values of the school and the safety of the learning environment, especially when ICT is used to facilitate misconduct.

5.2 Such a breach which is deemed harmful to the safety of the school (for example, involvement with inappropriate material, or anti-social activities like harassment), may constitute a significant breach of discipline and possibly result in serious consequences. The school will respond to any breach of the use agreement in an appropriate manner, taking into account all relevant factors, including contractual and statutory obligations.

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

5.4 Involvement with material which is deemed 'age-restricted', or 'objectionable' (illegal), under the Films, Videos and Publications Classification Act 1993, 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 in addition to any disciplinary response made by the school as a result of its investigation.

GENERAL CYBERSAFETY RULES –

The general rules have been developed to support the important school cybersafety initiatives outlined in Section A: Important Onslow College Cybersaftey Initiatives.

1 Use of any ICT must be appropriate to the school environment

1.1 For educational purposes only. The school's computer network, Internet access facilities, computers and other school ICT equipment/devices can be used only for educational purposes appropriate to the school environment. This rule applies to use on or off the school site. If any other use is permitted, the school will inform the user/s concerned.

1.2 Use of privately-owned/leased ICT equipment/devices on the school site, or at any school-related activity must be appropriate to the school environment. This includes any images or materials present/stored on privately-owned/leased ICT equipment/devices brought onto the school site or to any school-related activity. It also includes the use of mobile phones. Any queries should be discussed with the Cybersafety Manger, or with the Principal.

1.3 Responsibilities regarding access of inappropriate or illegal material.

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

- Initiate access to inappropriate or illegal material
- Save or distribute such material by copying, storing or printing

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

- Not show others
- Close or minimise the window or turn off the monitor (NOT the computer)
- Report the incident
    - Students should report to a teacher immediately
    - Staff should report such access as soon as practicable to the senior management.

2 Individual password logons (user accounts)

2.1 Individual user name and password. When Use Agreement forms are signed and returned, students will be issued with an individual user name and password to enable access to the school computer network, computers and Internet access using school facilities.

2.2 It is important to keep passwords confidential and it is prohibited to share your password with anyone else.

2.3 Users are not permitted to allow another person access to any equipment/device logged in under their own user account, unless with special permission from senior management. (Any inappropriate or illegal use of the Onslow College's computer facilities and other school ICT equipment/devices may be traced by means of this login information.)

2.4 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 this use 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 school environment. School email accounts must not be used to subscribe to sites, forward or contribute to chain letters or to send or receive attachments.

3 Disclosure of personal details

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

4 Care of ICT equipment/devices

4.1 All school ICT equipment/devices should be cared for in a responsible manner.

4.2 Any damage, loss or theft must be reported immediately to the Cybersafety Officer.

5 Wastage

5.1 All users are expected to practise sensible use to limit wastage of computer resource or band width. This includes avoiding unnecessary printing, and unnecessary Internet access, uploads or downloads.

6 Copyright and licensing

6.1 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.

7 Posting material

7.1 All material submitted for publication on the school Internet/Intranet should be appropriate to the school environment.
7.2 Such material can be posted only by those given the authority to do so by senior management.
7.3 The Cybersafety Officer should be consulted regarding links to appropriate websites being placed on the school Internet/Intranet (or browser homepages) to provide quick access to particular sites.

SECTION B – INFORMATION SPECIFICALLY FOR SECONDARY STUDENTS

1 The Student Cybersafety Use Agreement

1.1 You cannot use the school's computer network, Internet access facilities, computer and other Onslow College ICT equipment/devices until this Student Use Agreement has been signed by a parent/legal guardian/caregiver and signed by you, and the agreement has been returned to the school.

2 Use of ICT

2.1 While at school-related activity, you must not have involvement with any material or activity which might put yourself at risk. As well, you must not at any time use ICT to upset, harass, or harm anyone else in the school community, or the school 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. Behaviour the school may need to respond to also includes the use of websites to facilitate misconduct which puts at risk the safety of the school environment
2.2 If any privately-own ICT equipment/device, such as a laptop, PDA, mobile device, camera, or recording device, portable storage (like a USB or flash memory device). is brought to school for a school-related activity, the school cybersafety rules apply to that device. If you are not sure whether it is appropriate to have a particular device at school or at a school-related activity, you are expected to check with the relevant teacher before bringing it.

3 Consequences

3.1 The seriousness of a particular breach of the use agreement will have an appropriate response by the school. Possible responses could include one or more of the following: a discussion with the student, informing parents/legal guardian/caregiver, loss of student access to school ICT, taking disciplinary action. If illegal material or activities are involved, it may be necessary for the school to inform the police.

ADDITIONAL CYBERSAFETY RULES FOR STUDENTS –

1. Care of the computer and other school ICT equipment/devices, and their appropriate use includes:

- Use storage devices to back-up work or to take work home/back to school. (It is likely the school will need to check any storage device for such things as viruses.)
- Print material when in the classroom situation. Any material printed out of class must be appropriate in the school environment.
- Contribute material to the school Internet/Intranet site. As well, there should be no student involvement in any unofficial school Internet/Intranet site which purports to be representative of the school or of official school opinion.

2. Students must be considerate of other users. This includes:

- Sharing with other users and not monopolising equipment.
- 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.
- If you accidentally access inappropriate, dangerous or illegal material you should"
- Not show others
- Close or minimise the window
- Report the incident to a teacher immediately.
- You must have no involvement in any activity which could put at risk the security of the school computer network or environment. For example, no involvement with malware such as viruses or involvement with any form of electronic vandalism or theft.

It is our hope that with students following the conditions set out in this agreement. ICT will continue to be a valuable learning tool at Onslow College.