This document is comprised of this cover page and three sections:

Section A: Introduction
Section B: Cybersafety Rules for Secondary Students
Section C: Cybersafety Use Agreement Form.
Section D: Background Information for Parents

Instructions

1. Students and parents*/caregivers/legal guardians please read and discuss all sections carefully.
2. A copy of the document for future reference is available on the College website.
3. If you have any questions about this agreement please contact the school.

* The term ‘parent’ used throughout this document also refers to legal guardians and caregivers.

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 phones and MP3 players, iPods etc
(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, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use
(e) ‘Objectionable’ in this agreement means material that deals with matters such as sex, cruelty, or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school environment
SECTION A
Introduction

The measures to ensure the Cybersafety of Tranby College outlined in this document are based on our core values.

The school’s computer network, Internet access facilities, computers and other school ICT equipment/devices bring great benefits to the teaching and learning programmes at Tranby College, and to the effective operation of the school.

Our school has rigorous cybersafety practices in place, which include cybersafety use agreements for all school staff and students.

The overall goal of the school in this matter is to create and maintain a cybersafety culture which is in keeping with the values of the school, and legislative and professional obligations. This use agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cybersafety breaches which undermine the safety of the school environment.

All students will have a use agreement in their Student Organiser. Once signed by the student, parent and their form teacher, students will be able to use the school ICT equipment/devices.

The school’s computer network, Internet access facilities, computers and other school ICT equipment/devices are for educational purposes appropriate to the school environment. This applies whether the ICT equipment is owned or leased either partially or wholly by the school, and used on or off the school site.

SECTION B
Rules to Help Keep Tranby College Students Cybersafe

As a safe and responsible user of ICT I will help keep myself and other people safe by following these rules

1. I cannot use school ICT equipment until my parent and I have read and signed my use agreement form (see Section C) and returned it to school.

2. If I have my own user name, I will log on only with that user name. I will not allow anyone else to use my user name.

3. I will not tell anyone else my password.

4. While at school or a school-related activity, I will not have any involvement with any ICT material or activity which might put myself or anyone else at risk (e.g. bullying or harassing).

5. I understand that I must not at any time use ICT to upset, offend, harass, threaten or in any way harm anyone connected to the school or the school itself, even if it is meant as a joke.

6. I understand that I am not allowed to capture, publish or upload any images of members of the College community without their prior consent.

7. I understand that the rules in this use agreement also apply to mobile phones and iPods etc. I will only use my mobile phone or iPod etc at the times that I am permitted to during the school day.
8. I understand that I can only use the Internet at school when a teacher gives permission and there is staff supervision.

9. While at school, I will not:
   - Access, or attempt to access, inappropriate, age restricted, or objectionable material
   - Download, save or distribute such material by copying, storing, publishing, printing, or showing it to other people
   - Make any attempt to get around or bypass security, monitoring and filtering that is in place at school.

10. If I accidentally access inappropriate material, I will:

   1. Not show others
   2. Turn off the screen or minimise the window and
   3. Report the incident to a teacher immediately

11. I understand that I must not download any files such as music, videos, games or programmes without the permission of a teacher. This makes sure the school complies with the Copyright Act 1998. I also understand that anyone who infringes copyright may be personally liable under this law.

12. I understand that these rules apply to any privately owned ICT equipment/device (such as a laptop, mobile phone, USB drive) I bring to school or a school-related activity. Any images or material on such equipment/devices must be appropriate to the school environment.

13. I will not connect any device (such as a USB drive, camera or phone) to, or attempt to run any software on, school ICT without a teacher’s permission. This includes all wireless technologies.

14. I will ask a teacher’s permission before giving out any personal information (including photos) online about myself or any other person. I will also get permission from any other person involved. Personal information includes name, address, email address, phone numbers, and photos.

15. I will respect all ICT systems in use at school and treat all ICT equipment/devices with care. This includes:
   - Not intentionally disrupting the smooth running of any school ICT systems
   - Not attempting to hack or gain unauthorised access to any system
   - Following all school cybersafety rules, and not joining in if other students choose to be irresponsible with ICT
   - Reporting any breakages/damage to a staff member.

16. I understand that the school may monitor traffic and material sent and received using the school’s ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including email.

17. I understand that the school may audit its computer network, Internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit. Auditing of the above items may include any stored content, and all aspects of their use, including email.
18. I understand that if I break these rules or in any other way use ICT in a manner which is deemed as inappropriate by the College, the College may inform my parent(s). If deemed appropriate by the College, the College may take disciplinary action against me in line with the College’s Discipline Policy. I also understand that my family may be charged for repair costs. If illegal material or activities are involved, it may be necessary for the College to inform the police.

**TRANBY COLLEGE 6-12 CYBERSAFETY USE AGREEMENT FORM**

To the student and parent/legal guardian/caregiver, please:

1. **Read this page carefully** to check that you understand your responsibilities under this agreement
2. **Sign the appropriate section on this form**
3. **A copy of the document for future reference** is available on the College website.

We understand that Tranby 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 rules and requirements 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
- Welcome enquiries from students or parents about cybersafety issues.

Section for student

My responsibilities include:

- I will read this cybersafety use agreement carefully
- I will follow the cybersafety rules and instructions whenever I use the school’s ICT
- I will also follow the cybersafety rules whenever I use privately-owned ICT 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 school ICT. 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
- Referring to the document in my Student Organiser for clarification if I need to and/or
- I will ask a teacher if I am not sure about anything to do with this agreement.
TRANBY COLLEGE 6-12 CYBERSAFETY USE AGREEMENT FORM

Name of student: ......................................................... Class: ....................

Student’s signature: ......................................................... Date: ....................

Teacher's signature ......................................................... Date: ....................

Section for parent/legal guardian/caregiver

- I have read this Cybersafety use agreement and I am aware of the school's initiatives to maintain a Cybersafe learning environment, including my child's responsibilities.

My responsibilities include:

- I will read this cybersafety use agreement carefully and discuss it with my child so we both have a clear understanding of their role in the school’s work 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 child to follow the cybersafety rules and instructions
- I will contact the school if there is any aspect of this use agreement I would like to discuss.

I have read this cybersafety use agreement document and am aware of the school's initiatives to maintain a cybersafe learning environment, including my child's responsibilities.

Name of parent/caregiver/legal guardian: ..............................................................

Parent's signature: .............................................................. Date: ....................

(Please do not return this form as it will be in the student organiser, this your copy)
Dear parent(s)*,

This background information may be helpful as you read through and discuss the cybersafety use agreement with your son/daughter.

These are the seventeen rules to help keep students cybersafe as outlined in the cybersafety use agreement that you and your son/daughter have been asked to sign.

1. I cannot use the school ICT equipment until my parent and I have signed the use agreement and it has been returned to school.

All students must have a use agreement signed by themselves and their parent. Use agreements are an essential part of cybersafety policy and programmes for schools and other organisations.

2. If I have my own user name, I will log on only with that user name. I will not allow anyone else to use my user name.

The user name is the unique identity by which the network recognises an individual. There are never two users with the same user name and this allows the school to track the activity of any student. A user name could be misused if a student’s password was known and then used by others.

3. I will not tell anyone else my password.

Passwords perform two main functions. Firstly, they help to ensure only approved persons can access the school ICT facilities. Secondly, they are used to track how those facilities are used. Knowing how the equipment is being used and by whom, helps the school to maintain a cybersafe environment for all users, and teaches the student the importance of personal security.

4. While at school or at a school related activity, I will not have any involvement with any ICT material or activity which might put myself or anyone else at risk (e.g. bullying or harassing).

Unfortunately, along with many benefits, technology has also provided new ways to carry out anti-social activities such as bullying and harassment by text messages or on-line. Often students become involved in these acts through peer pressure, without thinking of the consequences.

5. I understand that I must not at any time use ICT to upset, offend, harass, threaten or in any way harm anyone connected to the school or the school itself, even if it is meant as a joke. This applies whether using ICT inside or outside of the school environment.

Harassing or bullying others will not be regarded as a joke by the school. Using sites such as msn, my space, facebook, or youtube etc outside of school to harass or bully other students or staff within the College will still be subject to the rules and expectations of this agreement.

6. I understand that I am not allowed to capture, publish or upload any images of members of the College community without their prior consent.

The publishing of images is potentially very harmful and hurtful to others and to the College community. This includes publishing images of oneself in College uniform or on College grounds.
7. I understand that the rules in this agreement also apply to mobile phones and iPods. I will only use my mobile phone or iPod at the times that I am permitted to during the school day.

Students and parents are also reminded of the school’s specific policy on the use of mobile phones at school.

8. I understand that I can only use the Internet at school when a teacher gives permission and there is staff supervision.

There must be an educational purpose for students to be online or accessing the Internet at school. Having a staff member present will help to ensure student safety.

9. While at school, I will not:
   a. Initiate access, or attempt to access age restricted, or objectionable material
   b. Download, upload, save or distribute such material by copying, storing, printing or showing to other people
   c. Make any attempt to get around, or bypass security, monitoring and filtering that is in place at our school.

The school has a number of steps in place to prevent students accessing inappropriate, age-restricted or illegal material. The students also have an individual role to play in this process by not attempting to access information they know will not be acceptable at school. Disciplinary procedures will result if a student is attempting to bypass school Internet filtering or security systems.

10. If I accidentally access inappropriate material, I will not show others. I will close or minimise the window and report the incident to a teacher immediately.

Because anyone at all can publish material on the Internet, it does contain material which is inappropriate, and in some cases illegal. The school has taken a number of steps to prevent this material from being accessed. However, there always remains the possibility that a student may inadvertently stumble across something inappropriate. Encouraging the student to tell a teacher immediately if they find something which they suspect may be inappropriate, encourages critical thinking and helps students to take responsibility for their actions and keep themselves and others safe. This way, they contribute to the cybersafety of the school community.

11. I understand that I must not download any files such as music, videos, games or programmes without the permission of a teacher. I also understand that anyone who infringes copyright may be personally liable under this law.

Many files available on the Internet are covered by copyright and although they can be easily downloaded, it may be illegal to do so. Sometimes these files can contain malicious content such as viruses, spyware programs or even inappropriate, age restricted or illegal material. As well, excessive downloading costs the College community money as well as potentially slowing the speed of the network for other users.

12. I understand that these rules apply to any privately owned ICT equipment/device (such as a laptop, mobile phone, USB drive) I bring to school or a school related activity. Any images or material on such equipment/devices must be appropriate to the school environment.

Students need to be aware that if they bring any ICT device to school or to a school related event, then all stored content on it must be acceptable and appropriate for the school environment.

13. I will not connect any device (such as a USB drive, camera or phone) to school ICT or run any software without a teacher's permission. This includes wireless technologies.

Connecting devices and installing software bought from home may cause conflicts with the school ICT systems. The school must also abide by software licensing requirements included with software. This means that if the school has not purchased the software, the school may not be legally entitled to install that software.
14. I will ask my teacher's permission before I put any personal information online. I will also get permission from the other person involved.

This reduces the risk of students being contacted by someone who wishes to upset or harm them, or use their identity for purposes which might compromise student’s privacy or security online.

15. I will respect all school ICT and treat ICT equipment/devices with care. This includes not intentionally disrupting the smooth running of any school ICT system, not attempting to hack or gain unauthorised access to any system, following all school cybersafety rules, not joining in if other students choose to be irresponsible with ICT, and reporting any breakages/damage to a staff member.

In addition to promoting student safety, the rules help the school to protect the considerable investments made in expensive ICT equipment. Intentionally disrupting ICT systems will be seen by the school as intentionally setting out to disrupt the learning of others.

16. I understand that the school may monitor traffic and material sent and received using the school’s ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data including email.

The school has an electronic monitoring system that has the capacity to record Internet use, including user details, time, date, sites visited, length of time viewed and from which computer/device. The school may also use filtering to restrict access to certain sites.

17. I understand that the school may audit its computer network, Internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit. Auditing of the above items may include any stored content, and all aspects of their use, including email.

In an audit, all material, files and emails could be checked by the school.

18. I understand that if I break these rules, the school may need to inform my parent(s). In serious cases the school may take disciplinary action against me. I also understand that my family may be charged for repair costs. If illegal material or activities are involved, it may be necessary for the school to inform the police.

Depending on the seriousness of the breach, possible school responses could include one or more of the following: a discussion with the student, informing parent(s), loss of ICT privileges, the family possibly having responsibility for repair/replacement costs, the school taking disciplinary action, involving the police.

*The term ‘parent’ used throughout this document also refers to caregivers and legal guardians.*
TRANBY COLLEGE CYBERSAFETY POLICY

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 and responsible use of the Internet and ICT equipment/devices, including mobile phones, mp3 players and iPods etc.

(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, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), Gaming Consoles, and any other, similar, technologies as they come into use.

Rationale

Tranby College has an obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the community. In addition Tranby College has a responsibility to be a good employer.

These three responsibilities are increasingly being linked to the use of the Internet and Information Communication Technologies (ICT), and a number of related cybersafety issues.

Tranby College places a high priority on providing internet facilities and ICT devices / equipment which will benefit student learning outcomes, and the effective operation of the school.

However, the College recognises that the presence in the learning environment of these technologies (some provided partly or wholly by the school and some privately owned by staff, students and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximise the benefits of these technologies, while at the same time to minimise and manage the risks.

Tranby College thus acknowledges the need to have in place rigorous and effective school cybersafety practices which are directed and guided by this cybersafety policy.

Policy

Tranby College will develop and maintain rigorous and effective cybersafety practices which aim to maximise the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimising and managing any risks.

These cybersafety practices will aim to not only maintain a cybersafe school environment, but also aim to address the need of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.
Policy guidelines

This policy should be read in conjunction with the College’s ICT Strategic Plan.

The Principal will report regularly to the College Council on issues pertaining to cybersafety and/or the use of ICT within the College.

Guidelines for Tranby College Cybersafety Practices

1. The school’s cybersafety practices are to be based on up to date information and are to be reviewed annually.

2. No individual may use the school Internet facilities and school-owned/leased ICT devices/equipment in any circumstances unless the appropriate use agreement has been signed and returned to the school. Use agreements also apply to the use of privately-owned/leased ICT devices/equipment on the school site, or at/for any school-related activity, regardless of its location. This includes off-site access to the school network from school or privately-owned/leased equipment.

3. Tranby College use agreements will cover all College employees, all students (including adult and community), and any other individuals authorised to make use of the school Internet facilities and ICT devices/equipment, such as teacher trainees, external tutors and providers, contractors, and other special visitors to the school.

4. The use agreements are also an educative tool and should be used as a resource for the professional development of staff as well as the on-going education of the students in matters pertaining to this area.

5. Use of the Internet and the ICT devices/equipment by staff, students and other approved users at Tranby College is to be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements.

6. Signed use agreements will be required of all members of the College community before individuals are authorised to make use of the Internet and ICT devices/equipment.

7. The school has the right to monitor, access and review all use. This includes personal emails sent and received on the schools computer/s and/or network facilities at all times.

8. The school has the right to audit at anytime any material on equipment that is owned or leased by the school. The school may also request permission to audit privately owned ICT devices/equipment used on the school site or at any school related activity.

9. Issues relating to confidentiality, such as sighting student or staff information, reasons for collecting data and the secure storage of personal details and information (including images) will be subject to the provisions of the Privacy Act 1998.

10. The safety of children is of paramount concern. Any apparent breach of cybersafety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the school’s cybersafety practices. In serious incidents, advice will be sought from an appropriate source, such as AISWA or a lawyer with specialist knowledge in this area. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.
One to One Laptop, MacBook Air & iPad Programme 2012
Definition of Fair Wear and Tear

1. Must be in a suitable condition for resale without diminishing the value below the normal fair market value for an asset of similar age and make.

2. Examples of normal wear include and are not limited to:
   - Light scratches on notebook casing.
   - Light wear on notebook palm rests.
   - Faded lettering on keys.
   - Removable stickers/labels.
   - Slight plastic colour fading.

3. Examples of normal wear would NOT include and are not limited to:
   - Missing keys.
   - Cracked casing, frame or lid.
   - Broken hinges or latches that do not close.
   - Non-removable stickers/labels.
   - Etching, excessive scratching and abnormal markings.
   - Pressure patches, burns and scratches on screens.
   - Major equipment discolouration, paint (including liquid paper) or other substances requiring more than light cleaning for safe handling and process for resale.
   - System does not boot up or systems passwords that prohibit diagnostic level program execution or testing.
   - Removal of serial number identification/product tags.

4. Any defects or damages covered under the manufacturer’s warranty should be dealt with and corrected prior to equipment return.

5. Damage that disfigures the notebook from its normal appearance and function would be deemed to diminish the value compared to a model of equal age and make without disfigurement. Charges for repairs will never exceed a contractually agreed full market value.