

TERANG COLLEGE

ICT

POLICY (Students)

1. RATIONALE

Terang College believes in the power of contemporary approaches to education, using modern and cutting-edge technology and programs to transform and enhance the way our students learn. At all times this technology needs to be used in a manner that ensures a safe and productive learning environment for all students.

2. AIMS

- 2.1. To ensure the available technology is used to enhance the learning of all students.
- 2.2. To ensure a safe and secure learning environment for all students.
- 2.3. To enhance learning by thinking, collaborating and creating through ICT.

3. IMPLEMENTATION

- 3.1 Issues, actions and decisions relating to this policy will take into account Department of Education and Training policies, memos, guidelines and circulars and Ministerial Orders and Acts.
- 3.2 For the purpose of this document the terms “technology” and “device” describe any personal or College owned electronic computers or devices including, but not limited to, desktop computers, laptops, netbooks, iPad, iPods and MP3 players. The College’s ICT policy will be achieved through the implementation of the following guidelines:
 - 3.2.1 Use of electronic devices is for educational purposes and has priority over other recreational purposes. As such students must not:
 - 3.2.1.1 use any other persons internet or network account.
 - 3.2.1.2 use abusive or obscene language in any communications.
 - 3.2.1.3 steal, or deliberately or carelessly cause damage to any equipment.
 - 3.2.1.4 interfere with or change any software settings on other people’s files.
 - 3.2.1.5 attempt to bypass or reduce network security, including the use of VPN apps.
 - 3.2.1.6 store, upload or download any unauthorised or inappropriate files, documents, images or videos.
 - 3.2.1.7 waste resources (e.g. paper, printing and internet downloads).
 - 3.2.1.8 send “spam” (bulk and/or unsolicited email).
 - 3.2.1.9 reveal personal information in any communications, including telephone numbers, addresses, passwords or images.
 - 3.2.1.10 knowingly infringe copyright.
 - 3.2.1.11 use technology outside of class including, before school, recess, lunch, and after school whilst on school grounds, unless on authorised wet weather days
 - 3.2.2 Computer hardware is expensive and sensitive equipment and must be treated carefully. Students must not:
 - 3.2.2.1 remove or relocate equipment without permission of the ICT Manager.
 - 3.2.2.2 vandalise equipment or furniture
 - 3.2.2.3 mark or deface any equipment.
 - 3.2.2.4 interfere with networking equipment
 - 3.2.2.5 eat or drink near any computer resources
 - 3.2.2.6 attempt to repair equipment, regardless of any real or supposed levels of knowledge.
 - 3.2.2.7 unplug cables or equipment.
 - 3.2.2.8 remove covers or panels.
 - 3.2.2.9 disable the operation of any equipment.
 - 3.2.2.10 undertake any actions that may result in the damage of computer equipment, knowingly or carelessly, in addition to those specifically outlined above.

- 3.3 Computer operating systems and software must be installed and configured correctly in order to operate. Students must not:
- 3.3.1 Delete, add or alter any configuration files.
 - 3.3.2 Copy any copyrighted software to or from any computer, or duplicate such software.
 - 3.3.3 Deliberately introduce any virus or program that reduces system security or effectiveness.
 - 3.3.4 Install or use any VPN apps on personal or College iPads
- 3.4 Networks are designed for the use of the student logged into a particular device at the time:
- 3.4.1 Network accounts are to be used only by the authorised owner of the account.
 - 3.4.2 Students finding devices that are logged on must log out immediately.
 - 3.4.3 It is the responsibility of students to make backup copies of their work.
 - 3.4.4 Students must not attempt to log into a school resource with any username or password that is not their own.
 - 3.4.5 Students must not reveal their password to anyone except ICT staff or a classroom teacher.
 - 3.4.6 Students are responsible for everything done using their logon credentials, and everything in their storage space/device.
 - 3.4.7 Students must not enter any other person's storage space/device or do anything whatsoever to any other person's files.
 - 3.4.8 Students must not intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.
 - 3.4.9 Students must not have any offensive or inappropriate media or files of any type, obscene file names, insulting material, more than 2 gigabytes of non-related school files on College storage space. Students must not have software or applications deemed as inappropriate by the College.
- 3.5 Internet access is expensive and has been provided to assist students in their education. Students are expected to abide by the following:
- 3.5.1 Students must only use the internet with permission and not in any unauthorised way.
 - 3.5.2 The use of the internet is not intended for entertainment purposes.
 - 3.5.3 Students must not deliberately enter, or remain in, websites containing objectionable material. This includes websites that contain;
 - 3.5.3.1 Nudity, obscene language or sexual discussion intended to provoke a sexual response.
 - 3.5.3.2 Violence.
 - 3.5.3.3 Information on or encouragement to commit a crime.
 - 3.5.3.4 Information on making or using weapons, booby-traps, dangerous practical jokes or 'revenge' methods.
 - 3.5.3.5 Gambling
 - 3.5.3.6 Any material student's parents or guardians have forbidden them to see.
 - 3.5.4 Students who encounter any such site must immediately notify a teacher or the ICT office.
 - 3.5.5 Social media should not be accessed or used during school time on any device, whether College owned or personal. Social media includes, but is not limited to, Facebook, Twitter, Instagram, Snapchat, and Tumblr by students.
 - 3.5.5.1 The Snapchat application is not permitted on any College owned device, as it poses a significant risk to child safety.
 - 3.5.6 YouTube can be a valuable educational resource however students must ensure;
 - 3.5.6.1 YouTube is only viewed for educational purposes at the direction of teaching staff.
 - 3.5.6.2 That no material is posted to YouTube.
 - 3.5.7 Real-time chat and instant message programs, applications or websites are not to be used by students as they pose serious risks to students well-being.
 - 3.5.8 Students must not use the internet for commercial purposes or for profit.
 - 3.5.9 Students must not use the internet to spread computer viruses or distribute or receive software that is not in the public domain.
 - 3.5.10 Students must not intend to break the law by attempting to guess a password or trying to gain access to remote computers, even if such attempts are not seriously intended to succeed.
 - 3.5.11 Students must appropriately and to the best of their ability ensure they are not breaking any copyright laws. Students should acknowledge sources of any material quoted directly including images and text.
- 3.6 Student devices
- 3.6.1 Students will ensure devices are bought to school everyday, fully charged, and in a condition that allows them to be used in the required manner.
 - 3.6.2 Students at Terang College will have 1:1 access to iPads from years 5 onwards.
 - 3.6.3 iPads can be purchased through the College or another retailer.
 - 3.6.4 The College will provide families with a payment plan for the purchase of an iPad.

- 3.6.5 The College will support families experiencing financial hardship by making College iPads available to those impacted students.
- 3.6.5.1 iPads borrowed by students must be returned to the office at the end of each school day. Failure to do so may result in the iPad being removed from the student.
- 3.6.6 Students in years 10 – 12 have the option to bring their own device (BYOD). Students bringing their own device;
- 3.6.6.1 must ensure the device is solely the property of the student/family
- 3.6.6.2 accept that all material on the device as well as material accessed using the College's network is subject to review by College staff at any time.
- 3.6.6.3 may need their device un-prepped from the College's network and management system.
- 3.6.6.4 must notify the ICT Team if they experience problems with either hardware or applications. If the issue is deemed to be one that is related to the College network or infrastructure, assistance will be provided. If an issue is deemed to be one that is related to a warranty issue or repair, unrelated to the College's infrastructure, the student/parent/guardian will be informed of the need for them to arrange for the device to be repaired.
- 3.6.6.5 need to ensure the device is suitably labelled so it can be identified from other devices.
- 3.6.6.6 ensure that the device has the required school programs and applications.
- 3.6.6.7 ensure the name of the device is not changed so the ICT Team can easily identify it.
- 3.6.6.8 will not 'Jailbreak' or install 'VPN' on their device.
- 3.6.6.9 may be required to perform updates to software on their device, such as operating systems, apps/program, regularly to ensure that the device is up to date to support learning at an optimal level.
- 3.6.6.10 may need their device re-imaged or factory restored as a result of application malfunction. In these instances the College cannot guarantee the retrieval of personal data.
- 3.6.6.11 need to ensure their device meets the minimum hardware and software requirements, as outlined below;

Operating System	Version	Device RAM
Apple	Mac OS: 10.10 +	4GB +
Windows	Windows 7, 8, 8.1, 10	4GB +

- 3.7 Electronic mail is a valuable tool for personal and official communication both within the College network and on the internet. Whilst using emails students:
- 3.7.1 ensure they use appropriate language and be polite in all communication.
- 3.7.2 do not be insulting, abusive, swear or use vulgarities.
- 3.7.3 should never write hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviour.
- 3.7.4 should never include obscene comments, threats, sexually explicit material or expressions of bigotry or hate.
- 3.7.5 should never reveal their personal address or phone numbers or the personal address or phone number of another student or member of staff.
- 3.7.6 should not send unsolicited mail to multiple recipients ("spam").
- 3.7.7 should not send very large attachments.
- 3.7.8 should not use email for any illegal, immoral or unethical purpose.
- 3.7.9 should not attempt to disguise their identity or the true origin of their email.
- 3.7.10 should not forge header messages or attempt to use any mail server for deceptive purposes.
- 3.7.11 should not use any mail program designed to send anonymous email.
- 3.8 There are occasions when it is appropriate and beneficial for students to have access to a mobile phone. The College however, discourages the bringing of mobile phones to school. Students need to ensure mobile phones do not disrupt the educational purpose and safe environment of the College:
- 3.8.1 Mobile phones brought to school must not be used in any manner or place that interferes with the normal routine and operation of the College. This includes:
- 3.8.1.1 Operating mobile phones as cameras unless instructed by a member of staff.
- 3.8.1.2 Taking photos or recording video of another person without their consent.
- 3.8.1.3 Making or sending harassing or threatening phone calls, text messages or images.
- 3.8.1.4 Using a mobile phone to cheat in exams or assessment.
- 3.8.1.5 Using mobile phones as substitute calculators.
- 3.8.1.6 Parents needing to contact students during school time must do so via the General Office.
- 3.8.2 Students are required to take full responsibility for the use and safety of their mobile phone during school times. Students are:

- 3.8.2.1 required to ensure their mobile phone is switched off (not on silent or vibrate) and out of sight during class times.
- 3.8.2.2 never to lend their phone to another student.
- 3.8.2.3 required to store their phones in a safe and secure manner and never leave in an unattended bag or change room.
- 3.8.2.4 encouraged to leave their mobile phones in the coordinators office at the beginning of the day for collection at the end of the day.
- 3.8.2.5 required to report any received inappropriate material and delete it.
- 3.8.2.6 required to respect the law prohibiting mobile phone use whilst driving, including making or receiving voice calls and sending or receipt of SMS messages or data of any kind
- 3.8.3 If a mobile phone is lost, stolen or damaged during school hours, the College cannot:
 - 3.8.3.1 Investigate phone thefts as they are extremely difficult to trace and the College does not have the resources to do so.
 - 3.8.3.2 Pay for any loss or damage occurred. The Department of Education and Training and the College do not hold insurance for personal property.
- 3.9 The College does not allow for the use of MP3 players, iPods or other portable music devices to be used in class, during study session or outside of class. Any such devices must also comply with the rest of this policy.
- 3.10 The College reserves the right to check mobile phones and digital devices for inappropriate images, videos, messages, software or content, if they are suspected to be on the device or are concerned for the well-being or safety of a student.
- 3.11 It is the responsibility of the College to:
 - 3.11.1 Provide training on the safe and appropriate use of technology and the internet and make that training available to everyone.
 - 3.11.2 Make students and parents aware of the College ICT policy and ensure all students and parents have read and signed the College's *Acceptable Use Agreement* at the beginning of each year.
 - 3.11.3 Provide a safe learning environment by maintaining filtering software on the College network.
 - 3.11.4 Take action to block the further display of offensive or inappropriate materials that has appeared on internet links.
- 3.12 Loss and damage of equipment.
 - 3.12.1 **iPad and Bring Your Own Device**
 - 3.12.1.1 All devices are covered by a manufacturer's warranty and/or insured at the time of purchase by the student and their parent/guardians. The College recommends a warranty that covers a two to three period of time. These warranties cover normal use of the device and manufacturing defects. It does not cover negligence, abuse or malicious damage.
 - 3.12.1.2 Any problem, damage loss or theft must be reported to the Year Level Managers and/or ICT Team.
 - 3.12.1.3 In the case of a suspected theft, the ICT Team must be notified. A police report by the family may be required. There is NO INSURANCE coverage supplied for devices by the College, and we recommend that you list this item on your own home contents insurance to provide additional protection.
 - 3.12.1.4 The College is not responsible for following up warranty or insurance claims for personally owned devices. Limited assistance may be provided where appropriate.
 - 3.12.1.5 Students may be held liable for payment of any costs associated with; deliberate or negligent damage to College owned loan devices that they use; damage to laptops and desktops sited in classrooms, if said damage is found to be by a deliberate act or negligence.
 - 3.12.2 **College Equipment**
 - 3.12.2.1 All devices are covered by a manufacturer's warranty or extended third party warranty. The length of the warranty depends on the type of device. These warranties cover normal use of the device and manufacturing defects. It does not cover negligence, abuse or malicious damage.
 - 3.12.2.2 Any problem, damage loss or theft must be reported to the Year Level Managers and/or ICT Team.
 - 3.12.2.3 Students may be required to replace lost or damaged devices or equipment.
 - 3.12.2.4 If a device is lost or damaged, the ICT Team will determine whether a replacement is required and/or whether the student retains the privilege of using ICT technology until the repairs are paid for.

- 3.12.2.5 If a device is lost or damaged and is not covered by the manufacturer's warranty and/or the school's insurance arrangements, the ICT Team may determine that the student is required to pay the costs associated with repair or replacement.
- 3.12.2.6 Students may also be held liable for payment of any costs associated with; damage to loan devices that they use; damage to laptops and desktops sited in classrooms, if said damage is found to be by a deliberate act and/or negligence.
- 3.13 All students are expected to abide by this policy and should be aware of the Commonwealth of Australia's Crime Act below and the penalties that may apply if they fail to do so. More than one penalty may apply for a given breach of the this policy. Serious or repeated offences will result in stronger penalties.
 - 3.13.1 Under the Commonwealth of Australia's Crime Act:
 - 3.13.1.1 A person shall not knowingly or recklessly use telecommunications supplied by a carrier to menace or harass another person.
 - 3.13.1.2 A person shall no knowingly or reckless use a telecommunications service supplied by a carrier in such a way as would be regarded by reasonable persons as being, in all circumstances, offensive
 - 3.13.1.3 The Commonwealth Crimes Act applies to the Terang College computer network and its internet access.
 - 3.13.2 Possible penalties include:
 - 3.13.2.1 Removal of email privileges
 - 3.13.2.2 Removal of internet privileges.
 - 3.13.2.3 Removal of storage space and network access
 - 3.13.2.4 Detention
 - 3.13.2.5 Paying to replace damaged equipment or compensate the College for stolen internet or printing credit
 - 3.13.2.6 Removal of electronic device or mobile phone.
 - 3.13.2.7 Other consequences as the College deems appropriate, which may include suspension or expulsion.
 - 3.13.2.8 Criminal charges may be laid with the police.
- 3.14 Both parents/guardians and students will be required to agree to the terms and conditions outlined in this policy at the beginning of each school year.

3 EVALUATION

- 4.1 This policy will be reviewed every three years as part of the College's Policy review cycle.

Approved by College Council on 20/08/2018