ST EDWARD'S COLLEGE
WHERE YOUNG MEN ACHIEVE

13 Frederick St, East Gosford, NSW 2250
(02) 4321 6400
info@stedwards.nsw.edu.au
www.stedwards.nsw.edu.au

Information and Communications Technologies (ICT) Policy

Introduction	The purpose of Information and Communication Technologies (ICTs) at St Edward's College is to: • enhance student learning opportunities • promote student achievement • support the professional work of staff • enhance the school's management information and business administration systems. The use of ICTs within school must be consistent with the mission, vision, and values of a Catholic school. Use should be responsible, legal, appropriate and for educational purposes and should follow the guidelines outlined in this policy. This policy applies to the use of all school related ICTs for educational purposes, whether provided by the school or the student.
Definitions	Information and Communications Technologies are any electronic device or related applications which allow users to record, send, access, or receive information, in textual, audio, image or video form. These may include but are not restricted to: • computer systems and related applications such as internet discussion forums, chat rooms • mobile phones • personal digital assistants (PDAs) • fax machines • printers • video or still cameras • audio recording devices • devices with high density storage • Next G broadband • social networking • iPhone software
Personal Learning Device (PLD)	From 2018, the College adopted a 1:1 personal device program. Each student is provided with a personal learning device (PLD) which is used throughout Years 7 and 8. The learning objectives for students include: • enabling students to use technology to further their learning, independently and in structured lessons • providing teachers with the opportunity to consistently construct learning experiences that are geared towards collaboration and connection • increasing student engagement Every student receives the same device and the levy for the PLD is itemised on the family's school fees account ($500 annually for 2018/2019). The cost includes the following items:

	• full onsite technical support for your son's PLD provided by a dedicated College Helpdesk
	• all textbooks included digitally on the PLD
	• PLD preinstalled with Office 365 suite
	• access to all student files anywhere, anytime via Office 365 OneDrive
	• protective laptop sleeve for improved safety while transporting the device to and from school
	• replacement devices available to ensure your son's continued participation in digital classroom lessons
	• accidental damage cover provided on each device which includes all physical damage e.g., cracked screens with an excess of $100 dollars required for each repair
	• coverage for Theft and Loss provided; parents will be required to complete a statutory declaration and include police report in the event of a theft; currently an excess of $200 dollars will be required for each claim.
	At the end of Year 8 students will be required to return this device and a new device will be issued at the start of Year 9 to be used throughout Year 9 and 10. The College currently maintains a Bring Your Own Device (BYOD) program for Senior students. Students will be permitted to use the device provided in Year 9 as their BYOD in Years 11 and 12.
Acceptable Uses of ICT	Students should: **Respect resources** Examples include: • use ICT equipment and resources for educational purposes under teacher supervision • follow teacher directions for accessing files, programs, email, and Internet resources • seek advice from a teacher before responding to online prompts • delete emails from unknown sources without opening any attachments as they may contain a virus. **Respect others** For example, students must: • respect the rights, beliefs, and viewpoints of others • follow the same standards of behaviour online as you are expected to follow in real life • follow the Netiquette guidelines for online communications at the end of the document • observe copyright rules by respecting the information, ideas, and artistic works of others • acknowledge the author or publisher of information from the Internet and not claim the work or pictures as their own. **Keep themselves safe online** For example:

ST EDWARD'S
COLLEGE
WHERE YOUNG MEN ACHIEVE

13 Frederick St, East Gosford, NSW 2250

(02) 4321 6400

info@stedwards.nsw.edu.au

www.stedwards.nsw.edu.au

	• keep their passwords and personal work secure; students are responsible for all actions performed using their username and password
	• use the Internet and email for educational purposes only
	• use school provided email accounts only
	• seek teacher advice before providing personal details online
	• always get teacher permission before publishing any personal information or photos online.
Unacceptable Uses	This document does not list all unacceptable uses of ICT but outlines the general areas that are unacceptable as well as prohibiting some specific uses. The following uses of ICTs are considered unacceptable:
	Personal safety
	Disclosure of personal information can expose users to inappropriate material, physical danger, unsolicited commercial material, financial risks, harassment and bullying, exploitation, unreliable information, nuisance, and sabotage. You should NOT:
	• send or post detailed personal information, images or audio about yourself or other people. Personal contact information includes home address, telephone or mobile number, school address, work address, email addresses, etc
	• meet with someone you have met online without your parent's/guardian's approval and participation.
	Illegal activities
	Students need to be aware that they are subject to laws relating to assault, trafficking and computer offences. An electronic audit trail may provide evidence of offences. You should NOT:
	• attempt to gain access to any computer system or service, to which you do not have authorised access. This includes attempting to log in through another person's account or accessing another person's files or emails
	• make deliberate attempts to disrupt other people's use of ICTs
	• make deliberate attempts to destroy data by hacking, spreading computer viruses or by any other means
	• engage in any illegal act, such as threatening the personal safety of others, arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, etc
	• install or use software which is not licensed by the school.
	Network security
	You should NOT:
	• use the ICT facilities without supervision by College staff
	• provide your password to another person or in response to a request via email (even if it looks like the email comes from someone you know)
	• go looking for network security problems, because this may be seen as an attempt to gain unauthorised access to the network

ST EDWARD'S
COLLEGE
WHERE YOUNG MEN ACHIEVE

13 Frederick St, East Gosford, NSW 2250

(02) 4321 6400

info@stedwards.nsw.edu.au

www.stedwards.nsw.edu.au

• log into blocked sites by first entering other approved sites i.e., anonymous proxy sites

• post information that, if acted upon, could cause damage to, or disrupt the network

• open e-mails from unknown sources.

Respect for privacy

You should NOT:

• re-post a message that was sent to you privately without the permission of the person who sent the message

• take photos, sound, or video recordings of people, including background figures and voices, without their permission

• distribute private information, including photos or recordings, about another person without their permission

Respect for others

You should NOT:

• make personal attacks on another person

• harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If someone tells you to stop sending them messages, you must comply with their request

• send or post any inappropriate or inaccurate information, comments, images, video or audio about other people or organisations

• send or post personal information about other people without their permission.

Respecting resource limits

You should NOT

• use ICTs for other than educational activities

• post or respond to chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people

• print material of a personal nature without permission and, if permitted, this printing will probably incur a charge

Plagiarism and Copyright

You should NOT:

• plagiarise works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user

• use material from the Internet in a manner which violates copyright laws

• access or use material from the Internet which relates to exam cheating or providing completed assignments

• copy or distribute any software or media

	Access to inappropriate material Messages sent using the school ICTs and attempts to access inappropriate material using the schools ICTs may be monitored and logged by the school and you should assume this monitoring is continuous. Some inappropriate material may be filtered or blocked by the school. You should NOT: • use ICTs to access material that: - is profane or obscene (pornography) - is illegal OR advocates illegal acts - advocates violence or discrimination towards other people • if you unknowingly navigate to a web site that contains material that may be considered offensive, you must clear the screen immediately and notify the teacher • download MP3's, MPEG's, and other large files without teacher permission • play games of any type including Flash games and installed programs • access social networking sites e.g., Facebook, Instagram, YouTube, AIM • participate in online chats, discussion groups or mailing lists not relevant to your education • access sites blocked by the school • access material which is not relevant to your education • use the school ICTs to purchase, order or sell any goods. A special exception may be made if the purpose of such access is to conduct educational research and the teacher approves access.
Notification	You should: • disclose to your teacher any messages you receive that are inappropriate or disturb you • notify your teacher or Pastoral Leader if you identify a possible security problem • immediately disclose accidental access to inappropriate material to your teacher or Pastoral Leader. This will protect you against an allegation that you have intentionally violated the School Acceptable Use Policy • notify your teacher or Pastoral Leader if you are offended by another person's use of ICT.
Consequences of Improper Use	Personal devices brought into school or to school activities may be taken and accessed if it is believed that: • there has been or may be a breach of the school rules or a school policy, or • there may be a threat of harm to themselves or to others or to system security If unacceptable files and/or content are found those files/content may be deleted, and disciplinary action may follow. Any other use considered improper will be recorded and may be subject to the following consequences: • loss of access privileges for a period determined by the Pastoral Leader • informing parents/carers

ST EDWARD'S
COLLEGE
WHERE YOUNG MEN ACHIEVE

13 Frederick St, East Gosford, NSW 2250

(02) 4321 6400

info@stedwards.nsw.edu.au

www.stedwards.nsw.edu.au

	• application of the school's Pastoral Care policy that may include detention, suspension, or exclusion • legal action.
Use of Laptop Computers by Students When at School	While we do not accept responsibility for electronic equipment that goes missing or is damaged, teachers and Pastoral Leaders usually attempt to locate missing items and investigate damage. An increase in the number of laptops will lead to an increase in the amount of time being spent by busy staff dealing with missing and damaged items.
Netiquette	Netiquette refers to the guidelines and etiquette for online communication. You should: • ensure that email and online messages are written carefully and politely. You should also try to keep messages short and precise • use appropriate language. Anything you post online is public • not use obscene, profane, rude, threatening, sexist, racist, disrespectful, or inappropriate language • check e-mail frequently and delete unwanted messages promptly • be cautious in using humour and satire as they can easily be misinterpreted • respect the rights, beliefs, and viewpoints of others • follow the same standards of behaviour online as you are expected to follow in real life • ensure Caps Lock is off when typing text, as typing in all capitals is equivalent to online shouting.