



### Introduction

Christ Church Grammar School (the School) is committed to providing its students and staff with the latest Information Communication and Technology (ICT) hardware, infrastructure and online services in order to effectively support and enhance the teaching and learning process within the School. The School believes that the resources are tools for life-long learning and that they can be effectively employed to:

- seek and expand knowledge,
- engage, create and collaborate,
- collect and analyse, and
- share and publish information

It is expected that students utilise the school's ICT facilities in a responsible, efficient, ethical and legal manner, while conforming to the guidelines in this document. If unsure about a particular activity and its acceptability, students should consult their tutor or the IT Helpdesk. By not conforming to the guidelines in this policy, students risk having disciplinary or legal action taken against them.

### Scope and definition of ICT

'Information and Communication Technology' or ICT means all computer hardware, software, systems and technology (including the Internet and email) and telecommunications devices in facilities that may be used or accessed from a school campus or connected to a school's communication network. This includes all parent-funded and personal devices whilst in use on the School campus or under supervision of CCGS Staff (including sporting events, excursions, camps and overseas trips).

Restrictions and policies are put in place to encourage a safe use of ICT within an educational context, to maximise educational outcomes and to ensure the safety of its staff, students and community members.

Principles of ICT usage are as follows:

- at Christ Church Grammar School ICT is provided for educational purposes only,
- the provision of ICT is a privilege and not a right. This privilege can be removed if school rules are broken,
- students using the school's ICT must not break State or Federal laws (a summary of these laws are an attachment to this Policy and form part of this Policy),
- the school has the right to check all written, graphic, audio and other materials created, produced, communicated, stored or accessed on devices accessed by its Students, including emails,
- students shall be made aware that access to ICT and in particular email and the Internet can expose them to inappropriate material or potential harm,

- students shall take personal responsibility when using the School's ICT services by protecting their personal information and data, maintaining the required level of security, respecting the privacy of others, respecting the legal boundaries of licensing and copyright, and using language appropriate to the school's expectations,
- students shall take personal responsibility when using the school's ICT devices by protecting and ensuring all equipment is treated with respect,
- whilst students are encouraged to explore and discover methods for utilising technology within the educational context, Christ Church Grammar School shall identify acceptable and unacceptable use of technology, email and internet systems and is committed to regularly updating this policy,

If these conditions are breached, students risk having disciplinary or legal action taken against them, or their Parent/Guardian.

## Student access to ICT facilities (Labs)

In all cases, students must have a supervising teacher present to use IT facilities. Students should use these facilities for school related work only. Gaming is NOT permitted on all systems and devices during school hours.

Students may access the IT facilities during the following times:

- during lunchtime when made available,
- after school,
- during free periods – with permission from IT Staff, and
- during private study – with permission from IT Staff & supervising Teacher.

## Acceptable use of ICT facilities and devices include:

- researching information relating to assessments,
- gathering specific information about subject/topics,
- emailing or electronically communicating with a teacher, other student or member of the community for assistance with school related work, and
- other teacher directed activities.

Students shall at all times exercise caution as to the quality and accuracy of the information they are accessing or transmitting as they bear the responsibility for the content.

## Unacceptable use of ICT facilities and devices include:

- the transmission any material in violation of any local, state, or federal laws,
- being party to or participating in hacking, spamming, phishing scams, denial of service attacks and acts of fraud,
- copying, downloading and/or sharing of commercial software or other media (eg music, videos or apps) in violation of federal copyright laws,

Document title: <b>ICT acceptable use and electronic communications (student)</b>	CRICOS: 00433G	<b>Page 2 of 10</b>
Custodian of document: <b>Director of ICT</b>	Date last updated: <b>October 23, 2019</b>	

- acts of plagiarism and/or breaching copyright laws, including software copyright and re-engineering software,
- the use of profanities, obscene or other language that may be offensive to another student, member of staff or member of the community, when using email, text messages (including iMessage), instant messaging clients and public forums such as social networks (eg Facebook and Twitter),
- being party to, participating in or failing to report acts of harassment, abuse, bullying, threats or acts which may be considered harmful either physically or emotionally to fellow students or others outside of the school community,
- committing any form of physical or digital vandalism,
- use for commercial trade, conducting private business matters or use for personal gain,
- use for all forms of gambling,
- accessing, transmitting or distributing pornographic or obscene content, networks or websites,
- knowingly creating and/or introducing electronic viruses or malware that can effect any system or network,
- accessing another student's account or device without their consent,
- accessing any staff member's account without their consent,
- taking, transmitting or distributing still or recorded images of any staff member or student without their documented consent,
- bypassing the network security at the school via portable wireless devices (including smartphones), proxies or tunneling,
- removing the school network connection software, policies, certificates or antivirus software tools from any school provided devices, and
- participation in any intentional/malicious damage towards ICT facilities or devices.
- committing any form of physical or digital vandalism to the device or its protective cover (including drawing, marking, scratching or ripping),
- carrying, transporting or using the device without the school provided protective cover,
- using the device contrary to Teacher's instructions during school hours (8:30am – 3:05pm). This includes accessing YouTube, social networks, instant messaging clients and playing games,
- using the device contrary to Parent or Guardian instructions after school hours. This includes accessing YouTube, social networks, instant messaging clients and playing games,
- shifting resource responsibility from the intended student to another individual (a student is always responsible for resources allocated to them),
- removing the school network connection, software, policies, certification or antivirus software from the device,
- willful breach of vendor warranty through unauthorised repairs or hacking (e.g. Jailbreaking) the operating system, software or applications, and
- bypassing the network security and filtering at the school via portable wireless devices (including smartphones),

proxies or tunneling.

## Digital etiquette

The following is a list of expectations students are to understand and accept when using school provided devices. Students are expected to:

- follow all teacher directions including when to use the device,
- have the volume of devices muted at the beginning of each lesson,
- use appropriate manners when communicating electronically,
- provide their device to teacher upon request, and
- provide their device to parents and guardians upon request.

## Digital access and device usage

Students are expected to utilise access to various communications offered by the School in an appropriate and safe manner conforming with:

- students are required to maintain and clean their device,
- students are required to report any damage immediately to the ICT Helpdesk,
- students are required to inform the teacher or others when using the camera and audio recording functions and are reminded that they must not publish photographs to any online network,
- students may not play games on their device between the hours of 8:30am and 3:05pm unless otherwise directed by a teacher,
- students are required to have the device fully charged and present at school at the beginning of every school day (with exception of sports events),
- when students are not required to have the device in class (eg for Sport) they should secure it in their locker and not leave it in the gymnasium change rooms,
- students are required to actively check their school email for communication from the School and their Teachers,
- students may not loan their device to another student or leave it in such a place that it is likely to be easily stolen or damaged,
- similarly, students may not use another students device unless necessary for a class activity or they have permission to do so from its owner,
- students must only download appropriately rated application, videos and music to the school device, and
- the device is and always will remain the property of CCGS and must be returned at the end of the loan period in working order.

## Digital health and wellbeing

Document title: <b>ICT acceptable use and electronic communications (student)</b>	CRICOS: 00433G	<b>Page 4 of 10</b>
Custodian of document: <b>Director of ICT</b>	Date last updated: <b>October 23, 2019</b>	

The elements of physical and psychological wellbeing related to digital technology use. A balance between the use of digital technologies and physical activities is essential. Students must commit to a healthy lifestyle by using mobile devices only when relevant during the school day, and should commit to a balanced use of the device at home.

## Device loss or damage

In the event of loss or accidental damage, students must report the incident to their teacher, tutor, Head of House or the ICT Helpdesk immediately.

In the event of theft or deliberate damage while at school you must report the incident to your teacher or the ICT Helpdesk immediately. Where this occurs, while not at school, you must report the incident to the police and then to the Director of ICT as soon as practical.

Parent/guardian of the student will be required to cover the cost of repairing/replacing the device due to loss or damage.

In the event where a third party is involved in an incident of damage, the matter will be referred to the student's tutors to resolve. Should no third party be identified the responsibility is placed on the student borrowing the device.

## Device overarching agreement

The student device is provided by the School and as such is subject to regular classroom / school disciplinary practices performed by staff during school. At home parents are given full authority on the use of the device.

In addition, it is the responsibility of the student to report and, where appropriate, remind their peers of the individual responsibilities when using their devices.

## Use of ubiquitous mobile electronic devices

Ubiquitous mobile electronic devices include mobile phones, iPods, iPads, PDAs, personal computers, video and digital cameras, personal wifi hotspots and graphic calculators.

Students are encouraged to use mobile electronic devices for educational purposes subject to the following guidelines:

- use of mobile electronic devices for communication with parents, staff and other students during classes time is not permitted unless directed by a teacher,
- mobile electronic devices can be used for communication during recess or lunchtime, however, outside of designated learning areas within the school,
- when in a classroom, students are required to keep their electronic device inaudible unless directed by a teacher,
- portable music devices are not to be used during the school day (from 8:15am until 3:05pm) unless directed by a teacher,
- earphones may only be used in teacher directed activities. Students are NOT allowed to walk around campus with earphones in or use earphones in designated learning areas at School,
- no calls or text messages are to be made or taken during class hours. Emergency calls by parents are to be directed to reception,
- the School will not be responsible for the loss, misuse or damage of privately-owned mobile electronic devices, or

any other valuables,

- mobile devices will be confiscated if the guidelines listed herewith are not followed. A parent or guardian may be required to collect them personally from the Head of House concerned. Other sanctions may be imposed if there is a recurrence of the issue, and
- students are expected to take the best care possible with school owned mobile devices, and report any damages or incidents to the ICT helpdesk.

## Residential students

Residential students are subject to the ICT acceptable use policy guidelines as with dayboys. In addition they are subject to the residential community ICT acceptable use policy found in the residential community handbook.

In general a boarding student who brings his own computer into the residential precinct needs to be aware of the following:

- the computer must have antivirus software installed as determined by the school. The antivirus profiles must be kept up-to-date. Students whose computers are infected with virus must 'clean' them immediately,
- additional monitoring systems are installed on the boarding network. Any boarder who attempts to bypass the network security systems, web filtering system and / or firewall will have his network access terminated for a period of one term,
- all inbound and outbound Internet traffic is logged. This included websites visited, email and chat sessions,
- each term there will be a random audit on a number of students own computers. This will involve a data search of the hard drive with a particular focus on inappropriate content, and
- the use of school provided mobile devices are also subject to these guidelines where applicable.

## Monitoring of ICT services and devices

All student mail and messaging is monitored for inappropriate content and language and is reported upon accordingly.

Student devices will be confiscated should they disrupt the learning of other students, be used inappropriately or if students take photos or videos of Staff members or other students without their explicit consent.

Student devices may also be confiscated and searched should the device contain inappropriate content or be involved in an incident of inappropriate behavior.

Personal restrictions and passcodes are to be placed on devices to protect personal data and unwanted use.

In the event of any misconduct on the part of the student ICT staff will require access to personal restrictions, passwords, passcodes and encryption.

## Student passwords

All students are issued with a unique password at the commencement of the academic year. These passwords are for the individual students use ONLY and as such they should not be given to any other student at the school. Students are responsible for protecting their individual password.

Sharing passwords could hold 'innocent' students liable in the event of misconduct and as such is strongly discouraged.

Document title: <b>ICT acceptable use and electronic communications (student)</b>	CRICOS: 00433G	<b>Page 6 of 10</b>
Custodian of document: <b>Director of ICT</b>	Date last updated: <b>October 23, 2019</b>	

Students who use another student's password will be deemed to be in breach of the schools acceptable use policy.

If a student suspects their password security has been breached they student should immediately report this occurrence to the ICT Helpdesk. A new password will be issued and further misuse of the password will be monitored and dealt with a necessary.

## File servers

Each student has been provided with an area on the file server or Cloud storage where he can save his documents; this is referred to as his folder. To access his folder the student must enter his name and password at login.

Some guidelines for student use of these folders:

- your folder is your own private folder,
- you should never access any other user's folder or device,
- you must never let any other user have access to your folder,
- you must never give any other student your password (including those of Social Networking Sites), and
- you must never attempt to find out another user's password.

## Email

Students are provided with their own email address for use at school in the format of:

[studentID@student.ccgswa.edu.au](mailto:studentID@student.ccgswa.edu.au)

Students can expect to have their email audited by IT staff on a regular basis. Students found to have been using these resources inappropriately can expect disciplinary action.

Students should be aware of the following expectations when using this system:

- students are expected to be sensible in their use of email. This includes NOT contributing to 'junk' or spam email,
- always consider your correspondence to be public. Even 'private' e-mail can get inadvertently routed or the recipient could forward copies anywhere,
- do not publicly criticise, anger or abuse others,
- be sensitive in what you write, and
- you should never reveal personal details such as your name or phone number to other via email or via the Internet

It is unlawful to send electronic messages, such as emails, which:

- defame someone or an organization,
- infringe copyright laws i.e. reproduce or adapt copyrighted material by downloading and further disseminating the material,
- contain statements which could constitute sexual discrimination or sexual harassment,

- display sexually offensive or explicit material,
- contain offensive or insulting statements based on race, colour or nationality of a person, and
- undertake activities that breach State and Commonwealth laws.

## Printing

Student should be aware of the following expectations:

- conserve paper – only print required documents,
- print only the exact number of copies required,
- avoid pressing print multiple times as there can be a delay when printing – always check the queue on the copier,
- remember that other people may be printing on the same printer as you, therefore make sure that you leave their work in the print tray,
- colour copying and printing can only be performed or released by staff, and
- ICT keeps a log of your printing – Please refrain from printing unnecessary or useless documents

## Internet usage

Students should be aware of the following expectations:

- the use of the Internet is for school related activities only,
- students are required to use the Internet responsibly – A rule of thumb for this: If I am looking at or doing something that would make me uncomfortable were it shared in my name with any teacher, fellow student or my parents, then I am making inappropriate use of the Internet,
- access to social networking sites, if permitted, is a privilege and not a right,
- students should not use the Internet to damage another persons' reputation (be it a fellow student, a member of staff, a student from another school, a parent or yourself),
- students are NOT permitted to use proxy sites to circumvent the filtering software, and
- all access to the Internet is monitored and logged – Please use it as an educative resource rather than a social/gaming network.



## Legal implications

Students are advised that the inappropriate use of electronic information can be a violation of local, state and federal laws. Please make yourself aware of the attached statutes that are applicable to your use of the Schools ICT facilities

### Copyright Act 1968 (Cth)

Students may copy or otherwise deal with copyright material for the purpose of study or education. However, generally only the author of original material has the right to reproduce, copy, publish, perform, communicate to the public and make an adaptation of the copyright material.

Reference: <http://www.comlaw.gov.au/Details/C2012C00835>

### Equal Opportunity Act 1984 (WA)

The objectives of the Act are to:

- a) to eliminate, so far as is possible, discrimination against persons on the grounds of sex, marital status, pregnancy, family responsibility or family status, race, religious or political conviction, impairment, age or, in certain cases, gender history in the areas of work, accommodation, education, the provision of goods, facilities and services, and the activities of clubs; and
- b) to eliminate, so far as is possible, sexual harassment and racial harassment in the workplace, and in educational institutions and sexual harassment and racial harassment related to accommodation; and
- c) to promote recognition and acceptance within the community of the equality of men and women; and
- d) to promote recognition and acceptance with the community of the equality of persons of all races, regardless of their religious or political convictions, their impairments or ages.

Reference: <http://www.eoc.wa.gov.au/about-us/equal-opportunity-act-1984>

### Censorship Act 1996 (WA)

Students must not use a computer service to transmit, obtain or request an article knowing that it contains objectionable and restricted material. It is an offence to possess or copy indecent or obscene articles or child pornography. Students should be aware for their own protections that people who deal with such material commit an offence.

Reference: [http://www.slp.wa.gov.au/legislation/statutes.nsf/main\\_mrtile\\_151\\_homepage.html](http://www.slp.wa.gov.au/legislation/statutes.nsf/main_mrtile_151_homepage.html)

### Criminal Code (WA)

Students should be aware that it is illegal to show offensive material to children under 16, and that if someone does show them offensive material that person is committing an offence. Racist harassment and incitement to racial hatred are also criminal offences.

Reference: <http://www.comlaw.gov.au/Details/C2012Q00003>

### Cybercrime Act 2001 (Cth)

Unauthorised access to or modification of data held in a computer and unauthorised impairment of electronic communication eg 'hacking' or infecting computer systems with a virus, are illegal

Reference: <http://www.comlaw.gov.au/Series/C2004A00937>

Document title: ICT acceptable use and electronic communications (student)	CRICOS: 00433G	Page 9 of 10
Custodian of document: Director of ICT	Date last updated: October 23, 2019	

## Privacy Act 1988 (Cth)

Students should respect that the personal information of others is private. This Act covers the collection, use and disclosure, quality and security of personal information.

Reference: <http://www.comlaw.gov.au/Series/C2004A03712>

Document title: <b>ICT acceptable use and electronic communications (student)</b>	CRICOS: 00433G	<b>Page 10 of 10</b>
Custodian of document: <b>Director of ICT</b>	Date last updated: <b>October 23, 2019</b>	