1. Purpose and Scope

Christ Church Grammar School (the School) provides its students with the latest Information and Communication Technology (ICT) hardware, infrastructure, software, and online services to support and enhance teaching and learning within its community.

This policy defines the core expectations of students when using any school provided ICT resources. These core expectations are based on the responsible, efficient, ethical and legal use of the ICT resources while maintaining the privacy, safety, security and wellbeing of the student body.

All Christ Church Grammar School, students who are provided with School supplied devices and/or access to the School's systems and/or network, including via personal parent-provided devices, are bound by the provisions of this policy. Students who breach the policy risk disciplinary action being taken against them.

This policy should be read in conjunction with the Code of Conduct for all Students.

2. Definitions

Information and Communication Technology (ICT) means all computer hardware, software, systems, infrastructure, services and telecommunication devices provided by the School. Additionally, it also includes all parent or personally owned devices used to connect or access the School's technology infrastructure while under the supervision of Christ Church Grammar staff (including in the boarding house, at sporting events, excursions, camps and overseas trips).

3. Policy Principles

3.1 General Provisions

- Christ Church Grammar School ICT resources are predominantly provided for educational purposes. All other use is considered as by exception and is susceptible to regular review.
- The School retains the right to withhold access to school ICT resources if students do not comply with the acceptable use of these resources.
- It is a condition of ICT use that the School reserves the right to inspect all content (e.g. written, graphic, audio, video, email etc.) created, produced, communicated, stored or accessed on all ICT resources or infrastructure (this includes personal devices used under the ICT definition above).
- It is a priority of the School to increase student awareness of the potential for exposure to inappropriate material and/or potential harm. Students should exercise caution as to the sites they are accessing and the quality and accuracy of the information they are transmitting.

3.2 Digital access, device usage and care

- Student devices are provided by the School and are subject to regular classroom/school disciplinary practices.
- Student devices are the property of the School and as such must be returned at the end of the loan period undamaged, in good working order with associated peripherals e.g. power, pen etc.

- In the event of loss, theft, accidental or deliberate damage, students must report the incident to their classroom teacher (where appropriate) or tutor during school hours, or the ICT Helpdesk after hours.
- The student's parent(s)/guardian(s) will be required to cover the cost of repairing or replacing the device due to loss or damage. Any repair/replacement costs that have the potential to be controversial must be discussed with the Director of ICT.
- Students are required to maintain and clean their device and have it fully charged at the beginning of every school day.
- When students are not required to have their device in class, it should be secured in the student's locker. Students should not leave their devices unattended, outside of the classroom unless it is in their locker.
- Students should not loan their device to another student, as any resulting costs due to damage or loss will be incurred by the lending student's parents or guardians.
- Students must not use another student's device unless authorised by a teacher or they have been granted permission from the owner of the device.
- Students must not wilfully damage, dispose or hide another student's device.
- Students must follow all teacher directions including when to use the device, have the volume muted at the beginning of each lesson and use appropriate etiquette when communicating electronically.
- Students are required to provide their device and password to their teachers, ICT staff, parents and guardians upon request.
- Students must inform the teacher when using the camera and audio recording functions and are reminded they must not publish photographs to any online network.
- Students must not play games on their device unless directed otherwise by a teacher.
- Students are required to check their school email and any other official school communication system such as Nexus or MS Teams periodically throughout the day at a time that does not interfere with regular classes.
- Students may only download approved applications and content (such as video, images, music, PDF etc.) to the school device via the school's software delivery mechanism.
- Devices should not be used during recess.
- During lunchtime, Senior School students are permitted to use devices in the School library, while use by students in the Preparatory School will be guided by teachers at all times.

3.3 Unacceptable use of ICT facilities and devices

- Being party to or participating in hacking, spamming, phishing, denial of service attacks and acts of fraud.
- Copying, downloading and/or sharing commercial software or other media (e.g. music, videos or apps) in violation of copyright laws.
- Acts of plagiarism including software copying and re-engineering software
- Use of profanities, obscene or other language that may be offensive to another student, member of staff or member of the community in email, text messages, instant messaging and public forums such as social media networks.
- Inappropriate use of Artificial Intelligence (AI).
- Being party to, or participating in, acts of harassment, abuse, bullying, threats or behaviour which may be considered capable of causing harm, physical, emotional or psychological, to another student, teacher, staff member or individuals in the community.
- Any forms of physical or digital vandalism.
- Unreasonable use for commercial trade, private business matters or personal gain.
- Any activities that have the capacity to negatively impact on student social, emotional and physical wellbeing (e.g., gambling).
- Access, transmission or distribution of pornographic or obscene content, networks or websites.
- Knowingly creating and/or introducing viruses or malware.
- Accessing another student' or staff member's account without their consent.
- Taking, transmitting, or distributing still or recorded images of a staff member or student without their documented consent.
- Bypassing the School's network security and/or filtering system e.g. proxies, tunnelling and / or hotspot access (mobile phone).
- Removing the School network connection software, policies, certificates or antivirus software.
- Participating in any malicious damage of ICT facilities or devices.
- Wilful breach of vendor warranty through unauthorised repairs or hacking (e.g., jailbreaking) the operating system, software or applications.

3.4 Access to ICT facilities/laboratories

- Students must have a supervising teacher present to use the ICT facilities/laboratories, and these should be used for school related work only.
- Students should not cause wilful damage to ICT facilities and/or equipment.
- Students may access the ICT facilities at the following times:
    - During lunchtime when available;
    - After school during ICT opening hours
    - During free periods with permission from ICT staff; and
    - During private study with permission from ICT staff and a supervising teacher.

3.5 Mobile Devices (phones, watches etc.)

- The School accepts no responsibility for the theft, loss or damage of student owned mobile devices.
- Mobile phones should be kept in the student's lockers and not in the possession of the individual student between 8.25am and 3.05pm (i.e., the school day).
- During school hours, no ear buds; headphones or ear pods should be seen outside of specialist rooms where teachers may explicitly allow for their use. This means it is at the discretion of individual teachers, as part of their learning processes, to allow for the playing of appropriate music and videos from mobile devices and computers. This also applies to private student classes for Senior School students.
- Use of a mobile device by a student during school hours may result in a staff member requesting the student to cooperatively and respectfully submit their mobile device. The staff member may either return the device after the lesson to the individual student, or the staff member may send the device to the student's Head of House or Student Services Co-ordinator (for Senior School Students), and the classroom teacher (for students in the Preparatory School), who will negotiate its return.

3.6 Residential students

Residential students are subject to the provisions of this policy. In addition, they are also required to adhere to the provisions of the ICT acceptable use policy for the residential community found in the Boarding Handbook.

A boarding student who chooses to bring his personal computer into the residential precinct is bound by 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 may become infected with a virus are required to "clean" them immediately.
- If using the School provided network or system, students should not attempt to circumvent the filtering or security system.
- All inbound and outbound internet traffic will be logged including websites visited, email and chat sessions.
- A random audit will be conducted each term on a random selection of student owned computers. This will involve a data search of the hard drive with a particular focus on inappropriate content.

3.7 Student passwords and space on the file server/cloud storage

- Students are issued with a unique password at the commencement of the academic year which they must reset as soon as possible.
- Passwords are for student's individual use only and not to be shared with any other student.
- Students who suspect their password security has been breached should immediately report this to the ICT Helpdesk. A new password will be issued, and the matter investigated by ICT.
- Each student is also provided with space on the file server/cloud storage for saving his documents. This is the individual student's folder with access provided via use of the student's name and password.
- Access to individual student folders is not to be shared with other students.

3.7 Email and internet protocols

- Each student is provided with an individual school email address.
- The provisions of this policy at section 3.1 and 3.3 are applicable to student use of the email system and the internet.
- Students should consider their correspondence to be public as emails may be forwarded by recipients.
- Students must be sensitive in what they write, refrain from criticism or abuse of others and never reveal personal details in an email or via the internet.
- Students are reminded not to infringe copyright laws or make statements which could constitute discrimination or harassment.
- Use of the internet is for school related activities only and a rule of thumb to be applied is "if I am looking at or doing something that would make me uncomfortable were it shared in my name with a teacher, fellow student or my parents, then I am making inappropriate use of the internet".

3.8 Printing

- Colour copying and printing can only be performed or released by staff.
- ICT maintains a log of student printing. Students are to refrain from printing unnecessary documents or copies of the same document.
- Students should avoid pressing print multiple times as there can be delays in printing.

4. Related Policies and Resources

Copyright Act 1968
Corruption and Crime Commission Act 2003
Cybercrime Act 2001
Human Rights and Equal Opportunity Commission Act (1986)
Western Australian Equal Opportunities Act (1984)
Work Health and Safety Act 2020(WA)
Privacy Act 1988
Code of Ethics
Code of Conduct for all Students
Privacy Policy
eSafety – Guidelines for social media use, video sharing and online collaboration