



Computer Network

Acceptable Use Policy

The Christadelphian Heritage College Sydney computer network is provided for staff and students to promote educational excellence by facilitating resource sharing, research and communication.

Students are provided access to the network with an individual account and internet access. Some students may also have college-administered individual email address. Student use of computer and network facilities may be monitored to ensure compliance with this policy document.

Any behaviour that interferes with these primary objectives will be considered an infringement of Acceptable Use. Infringements will be dealt with in accordance with the CHCS Discipline Policy. Penalties may range from a temporary ban on using computers, up to and including suspension or expulsion from the College. Criminal charges may be laid by the police where any laws are broken.

1. General

Appropriate use of the CHCS computer network includes:

- Using the resources and accessing materials for educational purposes as instructed by their teacher,
- Appropriate language must be used in all communications including email,
- Keeping computer areas clean and tidy.

Students must not:

- Use any other person's account,
- Consume food or drink or leave rubbish in computer areas,
- Use resources for the purposes of bullying, attacking, or intimidating any other person,
- Steal, or deliberately or carelessly cause damage to any equipment,
- Interfere with or change any software settings or other people's files,
- Knowingly infringe copyright including sharing copyrighted materials.



2. Computer hardware

Computer facilities are expensive, fragile and must be treated carefully.

Students are not to:

- Do anything likely to cause damage to any equipment or furniture,
- Eat or drink near any computer resources,
- Attempt to repair equipment without permission,
- Unplug cables or equipment, or relocate equipment without permission.

3. Software and operating systems

Computer operating systems and other software must be set up properly for computers to be useful. Each user has their own account which is only to be used by the authorised owner of the account. If you find a computer logged in, you should do nothing in that account except log out. Students are responsible for everything done using their accounts, and everything in their home directories. Since passwords must be kept secret, no user may claim that another person entered their home directory and did anything to cause college rules to be broken;

Students are not to:

- Change any computer settings (including screen savers, wallpapers, desktops, menus standard document settings, security settings etc) without permission,
- Bring or download unauthorised programs, movies, music or games to the college or run them on the network or share them, including running software from USB keys,
- Delete, add or alter any configuration files,
- Deliberately run or download any program or script e.g. virus that could reduce network security,
- Attempt to log into the network with any user name or password that is not their own, or change any other person's password,
- Reveal their password to anyone except the system administrator or classroom teachers, if necessary,
- Enter any other person's home directory or do anything whatsoever to any other person's files,
- Access or attempt to gain access to any restricted location on the network or any location not meant for student access,
- Create paths or gateways that allow them to repeatedly access locations or files that are not meant for student access.



4. Printing

The school has printing facilities for students and teachers to use, including the ability to do colour copying and printing. Student printing and copying is on a user pays basis to ensure the fair distribution of maintenance and running costs. Rates are available in the office. Each student will have an account which will receive an initial credit per term to cover the essential class materials. When the credit limit is reached printing and copying will be disabled until the account is topped up. Students must not attempt to bypass this system.

5. Mobile Phone use

Students are allowed to use mobile phones to listen to music on the bus to or from school. Once students enter the college, these devices must be switched off. If students need to contact anyone urgently, the office is available to make phone calls. Students are allowed to switch their phone on while at school only if they have the express permission of a teacher, and provided they turn it off again immediately afterwards. The college reserves the right to confiscate phones being used without permission.

6. Internet use

Internet access has been provided to assist students' education. Students must use it only with permission, and not in any unauthorised way. It is not intended for entertainment.

- Online or Real-time chat programs such as IRC, MSN and Windows Messenger are not to be used by students.
- Facebook and YouTube are not to be used by students unless they have the express permission of their teacher for a certain task.

Filtering technology is in place however it is the responsibility of individual students to ensure their behaviour is in line with the aims and ethos of the college. The college reserves the right to monitor online behaviour and track students' online activity.

Senior students are permitted to bring their own device to school for educational purposes only, provided:

- They complete the necessary paperwork which is signed off by the parent/carer and then the Principal,
- Bring their device in to be checked and registered by IT Support staff who will then sign off also,
- Receive a sticker approving the use of that device. This sticker must be clearly placed on the device and not removed.



7. Email & Online chat

Email is a tool used for personal and official communication both within the college network and on the Internet.

The following guidelines should be followed for students using email:

- Use appropriate language and be polite in your messages. Do not be insulting, abusive, swear or use vulgarities,
- Never write hate mail, chain letters, harassment, discriminatory remarks and other antisocial behaviours. Therefore, no messages should contain obscene comments, threats, sexually explicit material or expressions of prejudice or hatred.
- Do not reveal your personal address or the phone numbers of students or colleagues,
- Note that email is not guaranteed to be private. System administrators have access to all files including mail. Messages relating to illegal activities may be reported to the authorities,
- Teachers will set their own guidelines for use of electronic mail in class time.

8. Plagiarism

Taking ideas or writings from another person and offering them as your own is called plagiarism, and is an inappropriate use of College network. Credit should always be given to the person who created the article or the idea. The student should include their sources of ideas or writing e.g. the WWW address in the bibliography. The College is not responsible for the accuracy or quality of information obtained through use of the network. Use of any College owned computer is conditional on the acceptance of these terms. A disclaimer is displayed prior to login to reinforce this. Students are not to copy or distribute any copyrighted software or files to or from any device.

ACCOUNTABILITIES

Position	Accountabilities
All students	Students must abide by the College's policies
Parents/carers	<ul style="list-style-type: none">▪ Support and assist the school and their child/ren to uphold the College's policies

DEFINITIONS

Term	Definition
Nil	



Heritage College Sydney

wisdom through knowledge

REFERENCES

Documents that should be referred to in conjunction with this Policy are listed below:

Document Type	Title
Legislation	
Code of Practice	
Standards	
Other Policies	Technology – Student Use Policy
Guide	
Forms	General Permission and Computer Consent, Enrolment Commitment

DOCUMENT CONTROL

1. Ownership and Approval

Role	Name	Position title	Date
Author	John Unwin	Business Manager	Dec 2018
Approver	Felicity Shields	Principal	Dec 2018

2. Review

Stage	Date
Original Policy	
Policy revised	Dec 2017
This review	Dec 2018
Next review	Dec 2019

Date Created:

Management (M):\Business\Policies\General\