# ICT and Internet Acceptable Use Policy

| | |
|---|---|
| **Document Type:** | ICT and Internet Acceptable Use Policy |
| **Policy No:** | 24 |
| **Date of First Issue:** | April 2017 |
| **Last Review Date:** | May 2023 |
| **Document Author:** | Principal |
| **Authorised By:** | Committee of Management |
| **Next Review Date:** | May 2026 |

**Introduction**

The use of Information and Communications Technology (ICT) at Northside Christian College is incorporated in almost every aspect of our teaching and learning programs. At Northside Christian College, we promote the responsible, reliable and respectful use of ICT. This policy has been developed to assist the College community to use a whole range of technologies appropriately. The ICT and Internet Acceptable Use Policy addresses relevant moral, legal and professional issues.

**Aims**

- To ensure safe and responsible use, and ongoing care of all our ICT resources.

- To safeguard safety in an online environment.

- To improve student learning outcomes by increasing access to world-wide information.

- To develop skills to discriminate and apply appropriate Internet and computer usage.

- To encourage and promote ethical digital citizenship and cyber safety.

**Definitions**

For the purpose of this policy, Information and Communications Technology (ICT) is defined as being any electronic device or application which allow a user to access, receive, record, or send information, as text, images, audio, or video.

**Rationale**

The purpose of this Policy is to ensure that all use of Northside Christian College ICT resources is legal, ethical and consistent with the aims, values and objectives of Northside Christian College and its responsibilities to the students in its care. Northside Christian College is an institution charged with the safety and education of children. It also has occupational health and safety obligations to employees and students and must comply with State and Federal anti-discrimination and sexual harassment laws. It is therefore important that its ICT resources are used appropriately and professionally at all times.

The Northside Christian College ICT resources must be properly and efficiently used. The Northside Christian College resources are not to be used for inappropriate activities for example, pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment, including sexual harassment, stalking, privacy violations and illegal activity, including illegal peer-to-peer file sharing.

Northside Christian College provides access to the Internet for students and staff. The College provides ICT facilities for its students essentially for educational purposes related directly to their courses of study. The College's ICT facilities are not provided for social or recreational purposes. The College values the development of online resources for the purposes of supporting and extending students' learning.

The College does, however, recognise that the Internet provides access to the World Wide Web, which contains material inappropriate for school and student use. Whilst care is taken to ensure that students will use the Internet for positive education outcomes, including blocking and screening known objectionable sites, the College cannot guarantee that students will not find ways to access offensive or inappropriate materials.

The College reserves the right to monitor all files, emails and Internet activity taking place on the College's computer network.

In summary, this means users of the College's ICT resources are trusted to:

- Use College ICT facilities only for educational or work purposes.

- Never use the computer facilities to do anything illegal, fraudulent or deceptive.

- Never create or access offensive materials intentionally.

- Not use other chat or social network sites, unless it is by special arrangement with a teacher who has organised it for specific educational purposes. Please also refer to the College's Social Media Policy for additional guidance.

- Never use another person's log-in and password and keep their own password confidential.

- Not to establish Virtual Private Networks (VPNs) to bypass the College network.

**Scope**

This Policy applies to all users of the Northside Christian College ICT resources regardless of work location and applies to all aspects of use of all Northside Christian College ICT resources, for example:

- Publishing and browsing on the Internet;

- Downloading or accessing files from the internet or other electronic sources;

- Email;

- Electronic bulletins/notice boards;

- Electronic discussion/news groups;

- Weblogs ('blogs');

- Social networking;

- File transfer;

- File storage;

- File sharing;

- Video conferencing;

- Streaming media;

- Instant messaging;

- Online discussion groups and "chat" facilities;

- Subscriptions to list servers, mailing lists or other like services;

- Copying, saving or distributing files;

- Viewing material electronically; and

- Printing material.

Any reference in the list above can be amended from time to time.

**Implementation**

- The College actively supports access by students to the widest variety of information resources available, accompanied by the development of the skills necessary to filter, analyse, interpret and evaluate information encountered.

- Student behaviour when using College computers, iPads and networks, when using the Internet and e-mail, and when engaging in any activity with College computers must be consistent with this policy and the agreements in Appendix B.

- Signed parent and student consent (see Appendix B) is required to be completed in order to gain access to the Internet, or to publish work, photos or videos using the Internet.

- The consent form is expected to be signed by all students at the College. A student will only be allowed to access the Computer Network/Internet upon receipt of a consent form signed by both the student and a parent or carer.

- Privacy of students, parents, staff and other users must be recognised and respected at all times. Students will only identify themselves on the Internet by their first name and last initial.

- Staff are expected to utilise and integrate technologies, including on-line learning opportunities, into their programs for all students. Flipped learning is an essential pedagogical approach at Northside, which involves publishing pre-learning resources online for students.

- The College will provide appropriate professional development and support for all staff.

- Internet access and usage of College ICT facilities is an integral part of the College curriculum. Improper use, however, will result in the suspension of access at any time by the class supervising teacher or other member of staff. Repeated or severe misuse may also result in further disciplinary action being taken by the College.

The following are deemed, by example, as acceptable uses of the Internet for students within the College:
- To access learning resources on the College's Learning Management Systems.

- To research material for specific class projects.

- To supplement course materials and information.

- To research career choices.

- To undertake quality self-discovery activities related to, e.g. a hobby (only if the machine you are using is not required by another student for legitimate educational purposes).

**Use of the Schoology, myEdOnline and Web-based Systems**
Schoology and myEdOnline can be accessed through the College Network whilst at the College or remotely from home through a student's own Internet connection.

Learning Management Systems and online applications are provided and hosted by third parties; the content and operation of these systems are not fully controlled by the College. The use of these websites may be governed by the third party provider's terms of use and students must comply with such terms when using the site. The College may be required to create a student log-in for these websites, which will include the disclosure of their name and College email address.

**Student Guidance About Digital Citizenship**
A Digital Citizen is defined as a person who is a frequent user of information and communication technologies. A Digital Citizen has the same rights and responsibilities as a citizen in the 'real world'. Operating and communicating in the digital world leaves a digital footprint, a permanent reminder of our actions, inactions and interactions. Students at Northside Christian College are expected to apply the same principles of good citizenship to their interactions online.

The following guidelines are expected to be followed.

<u>Respect Yourself</u>
Select names and images that portray you in a positive light. Do not post any information that you would not want your family or employer to see.

- I will show respect for myself through my actions.

- I will select online names that are appropriate.

- I will consider the information and images that I post online.

- I will consider what personal information about my life, experiences, experimentation or relationships I post.

- I will not be involved in obscene language or behaviour.

<u>Protect Yourself</u>
Set the privacy settings on your tools to control access to your updates, posts or profile. Be sure of the facts you post. It's easy to send an email or post a message, in a moment of high emotion, but once sent it is almost impossible to delete. Think before you post.

If you are meeting someone you have met online in the real world, discuss it with people you trust, parents, friends, teachers etc. and never meet them alone.

- I will ensure that the information, images and materials I post online will not put me at risk.

- I will not publish my personal details, contact details or a schedule of my activities.

- I will report any attacks or inappropriate behaviour directed at me.

- I will protect passwords, accounts and resources.

<u>Respect Others</u>
As a responsible Digital Citizen, you model respect for other people. If you gossip or attack a person online, the potential audience is immense. A good general rule to follow is: If you would not say it in person, do not say it online. If you have nothing nice to say, then say nothing. Do not forward it, do not visit it, and do not condone it. You may not be in the same room as another, but you are not anonymous.

- I will show respect to others.

- I will not use electronic mediums to defame, bully, harass or stalk other people.

- I will show respect for other people in my choice of websites.

- I will not visit sites that are degrading, pornographic, racist or inappropriate.

- I will not abuse my rights of access and I will not enter other people's private spaces or areas.

<u>Protect Others</u>
We can protect others by not tolerating, and reporting behaviour that is inappropriate or unacceptable. Do not forward emails that are derogatory, delete them. Have a policy of zero tolerance for unacceptable behaviour. Consider what it would feel like if you were the recipient of such activity.

- I will protect others by reporting abuse, not forwarding inappropriate materials or communications; and not visiting sites that are degrading, pornographic, racist or inappropriate.

**Student Acceptable Use of Email Facilities**
All students have access to a College email account. Students should always use polite and considerate language when using email facilities to send and receive messages. Sending any personal information (full name, address, phone numbers, etc) via the College email

system is strictly forbidden. If students should receive a message via email, which makes them feel uncomfortable, they are to immediately tell a teacher.

**Cyber Abuse**
*The Online Safety Act 2021* (Cth) includes a world first scheme to take down cyber abuse and protect children and adults from online bullying. Bullying and harassment are also addressed in the College's Student Anti-Harassment and Bullying Policy. Harassment and bullying in any form are not tolerated at Northside Christian College.

**Defamation**
Northside Christian College ICT resources must not be used to send material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or Northside Christian College liability. Electronic communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and widespread.

**Copyright Infringement**
The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files, music files, video files, text and down loaded information) must not be used without authorisation to do so. The ability to forward and distribute electronic messages and attachments and to share files greatly increases the risk of copyright infringement. Copying material to a hard disk or removable disk, printing or distributing or sharing copyright material by electronic means, may give rise to personal and/or Northside Christian College liability, despite the belief that the use of such material was permitted.

Northside Christian College supports the rights of copyright owners and does not and will not tolerate reckless or deliberate copyright infringement.

**Illegal Use and Material**
Northside Christian College ICT resources must not be used in any manner contrary to law or likely to contravene the law. Any suspected offender will be referred to the police or other relevant authority. For staff, this may result in their employment being terminated.

Certain inappropriate, unauthorised and non-work-related use of College's ICT resources may constitute a criminal offence under the *Crimes Act 1958* (Vic), for example, computer 'hacking' and the distribution of computer viruses.

Illegal or unlawful use includes but is not limited to use of certain types of pornography (e.g. child pornography) under the *Crimes Act 1958* (Vic), offences under the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic), defamatory material, material that could constitute racial or religious vilification, unlawfully discriminatory material, stalking, blackmail and threats under the *Crimes Act 1958* (Vic), use which breaches copyright laws, fraudulent activity, computer crimes and other computer offences under the *Cyber Crime Act 2001* (Cth) or *Crimes Act 1958* (Vic) (as amended by the *Crimes (Property Damage and Computer Offences) Act 2003* (Vic)), or any other relevant legislation.

In particular, Northside Christian College is an institution charged with the safety and education of children. Child pornography represents the antithesis of the College's responsibilities to children. Any suspected offender will be referred to the police. For staff, their employment will be terminated if the allegations are substantiated.

**Offensive or Inappropriate Material**
Use of Northside Christian College ICT resources must be appropriate to a workplace environment. This includes but is not limited to the content of all electronic communications, whether sent internally or externally.

Northside Christian College ICT resources must not be used for material that is pornographic, harassing, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening. This includes sexually-oriented messages or images and messages that could constitute sexual harassment.

All users of College's ICT resources should be familiar with current anti-discrimination, equal opportunity and harassment policies legislation.

Users of the College's ICT resources who receive unsolicited offensive or inappropriate material electronically should delete it immediately. Offensive or inappropriate material received from people known to the receiver should be deleted immediately and the sender of the material should be asked to refrain from sending such material again. Such material must not be forwarded internally or externally or saved onto the Northside Christian College ICT resources except where the material is required for the purposes of investigating a breach of this policy.

**Confidentiality and Privacy**
Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of Northside Christian College ICT resources, users must be aware that this security is not guaranteed, particularly when communicated to an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

In relation to communications relating to the disclosure of improper conduct either as part of an audit or as contemplated by the *Whistleblowers Protection Act 2001* (Vic), it is advised that personal, not Northside Christian College, email accounts or other means of communication are used to report this information to maintain confidentiality.

Northside Christian College will handle any personal information collected through the use of Northside Christian College ICT resources in accordance with the *Information Privacy Act 2000* (Vic).

Northside Christian College will not disclose the content of electronic communications created, sent or received using Northside Christian College ICT resources to third parties outside of Northside Christian College unless that disclosure is required for the purposes of a Northside Christian College investigation, a police investigation or for other legal, investigative, audit or compliance reasons or in other circumstances where that disclosure does not contravene the *Information Privacy Act 2000* (Vic).

**Malware**
Electronic and web communications are potential delivery systems for computer malware. All data, programs and files which are downloaded electronically or attached to messages should be scanned by an anti-virus program before being launched, opened or accessed.

Malware has the potential to seriously damage Northside Christian College ICT resources. Do not open any attachments or click on any links embedded in an email unless you have confidence in the identity of the sender.

**Attribution**
There is always a risk of false attribution of breaches of this Policy. It is possible that communications may be modified to reflect a false message, sender or recipient. In these instances an individual may be unaware that he or she is communicating with an impostor or receiving fraudulent information. If a user has a concern with the contents of a message received or the identity of the publisher of the electronic information, action should be taken to verify their identity by other means. If a user believes an electronic communication has been intercepted or modified, the Deputy Principal or Principal should be informed.

Users are accountable for all use of Northside Christian College ICT resources that have been made available to them or leased to them for work purposes and all use of Northside Christian College ICT resources performed with their UserID. Users must maintain full supervision and physical control of Northside Christian College ICT resources, including notebook computers, at all times. UserIDs and passwords must be kept secure and confidential. Users must not allow or facilitate unauthorised access to Northside Christian College ICT resources through the disclosure or sharing of passwords or other information designed for security purposes.

Active sessions are to be terminated when access is no longer required and computers secured by password when not in use.

**Mass Distribution and 'SPAM'**
The use of Northside Christian College ICT resources for sending 'junk mail', for-profit messages, or chain letters is strictly prohibited. Mass electronic communications should only be sent in accordance with normal Northside Christian College procedures. The use of electronic communications for sending unsolicited commercial electronic messages ("Spam") is strictly prohibited and may constitute a breach of the *Spam Act 2003* (Cth).

**Archives**
Electronic communications are public records and subject to the provisions of the *Public Records Act 1973* (Vic). Northside Christian College record management practices for management of email messages must comply with Northside Christian College policies and guidelines on recordkeeping and management of electronic communications as amended from time to time. Please refer to the College's Records Management Policy.

Email messages that are routine or of a short term facilitative nature should be deleted when reference ceases, as distinct from ongoing business records such as policy or operational records.

**Disclaimer**
All emails sent externally from Northside Christian College email service will automatically have a disclaimer attached to them. The disclaimer must not be altered or interfered with in any way. The use of the disclaimer may not necessarily prevent Northside Christian College or the sender of the email from being held liable for its contents. School email systems must also append the same disclaimer to messages sent externally from the school's email service.

**Complaints**
If you wish to make a complaint or report about inappropriate use of Northside Christian College ICT resources raise it with the Principal or sub-school Director of Learning or, if your Principal is the cause of your complaint, raise it with a member of the College Committee of Management.

**Child Safe Standards**

On the 1st July 2022, the new Child Safe Standards came into force, along with new *Ministerial Order 1359*. Both instruments have an increased focus on child safety in the online environment.

Northside Christian College is commitment to implementing a broad range of strategies to mitigate risks to children and young people in online environments, including:

- Informing students and their families about appropriate use of the school's technology, safety tools and how to seek help and report concerns including cyberbullying and online grooming.

- Keeping up to date with current online safety issues and expert information from specialist government and non-government bodies including the Office of the eSafety Commissioner, and eSmart Schools.

- Promoting activities in the school community that connect schools and communities and raise awareness to prevent bullying and violence (e.g. National Day of Action against Bullying and Violence).

- Using filtering software on school-based devices.

- Encouraging parents to use parental controls on personal devices.

- Monitoring online activity and respond to breaches of the online policies and procedures with appropriate consequences.

- Informing students about online safety risks, including:
    - cyberbullying and trolling.
    - invasion of privacy or digital surveillance.
    - inappropriate sharing of images.
    - phishing, harvesting of personal information or data theft.
    - identity theft.
    - malevolent software (malware).
    - offensive images and messages.
    - age-inappropriate online content.
    - impersonation/catfishing.
    - grooming.

**Responsibilities**

Students

Students are responsible for their own good behaviour relating to all uses of College ICT facilities. They must act in accordance with the agreements outlined in Appendix B. Communications and activities on the information networks provided by the College are subject to the same rules that govern student conduct and standards of communication.

Students are subject to the College's Behaviour Management Policy and Student Code of Conduct when using ICT resources (whether accessing or using them from school, home or elsewhere).

Students and families in possession of College owned devices (including but not limited to laptops, cameras, digital cameras, video cameras, projection devices and hand held devices) are guided by the relevant College policies stated in this document.

Parents and Carers
Parents and carers are ultimately responsible for setting and conveying the standards that their children should follow. The College expects that those standards will be in accordance with College rules and the Student Code of Conduct, the student ICT agreements, this policy and other College policies.

Staff
The College expects that staff will incorporate appropriate use of such information throughout the curriculum and that teachers will provide guidance and instruction to students in the appropriate use of such resources. This will include staff facilitating students accessing information in support of and to enrich the curriculum while taking into account the varied instructional needs, students with disabilities, gifted and talented students and development levels of the students.

College staff are also expected to adhere to this policy document and other related policies. Teachers are expected to set standards that are in the best interests of learning and responsible use of technology as outlined in the relate policies and documents.

Staff should regularly update and improve their ICT skills as a matter of professional learning and endeavour to utilise electronic learning resources where appropriate. This includes maintaining a balanced approach to use of technology with the philosophy that digital devices are just one of a number of learning tools in the teaching and learning repertoire and therefore its use should be balanced and predicated on sound educational thinking.

Principal
The Principal undertakes a commitment to implement and uphold the ICT and Internet Acceptable Use Policy and to provide appropriate physical and financial resources to enable safe, educationally relevant access to the Internet and other ICT resources for staff and students.

The College undertakes to ensure that information published on the College network or the Internet by students or the other members of the College community under the College's name meets legal requirements and standards of general practice within the community in relation to copyright and safety.

**Student Breaches of the ICT and Internet Acceptable Use Policy**
All students at Northside Christian College have a right to use the ICT facilities available to them. They also have a responsibility to use it sensibly and maturely, and treat equipment and others with respect. Should students not do this; the following system of penalties will be applied as appropriate.

First Offence          Verbal warning to student.

Second Offence         One week suspension from using ICT facilities within the College.
                       Parents are notified.

Third Offence          One week suspension from using any ICT facilities within the College.
                       Possible other consequences are deemed appropriate in the College's
                       Behaviour Management Policy.

Fourth Offence         Meeting with parents. Possible suspension from use of ICT facilities
                       for the remainder of the Term in which the offences occurred. Possible
                       other consequences are deemed appropriate in the College's
                       Behaviour Management Policy.

**Note:** That should a deliberate or particularly offensive act occur, Steps 1 – 3 may be bypassed. All offences and actions taken will be reported to the Principal and the sub-school Director of Learning.

Limitations can be placed on an individual student's user privileges.

Where there is a reasonable belief that illegal activity may have occurred Northside Christian College may report the suspected illegal activity to the police.

**Staff Breaches of this Policy**
Staff breaches of this Policy may be categorised using the following categories. The categories do not cover all breaches of this Policy, for example the categories do not specifically refer to breaches of copyright. Matters not covered by the following categories will be dealt with on an individual basis and on the relevant facts.

Category 1: Illegal
This category covers the following:

a. Child pornography – offences relating to child pornography are covered by the *Crimes Act 1958* (Vic) and the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic). Child pornography is defined in section 67A of the *Crimes Act 1958* (Vic) as:

> "a film, photograph, publication or computer game that describes or depicts a person who is, or appears to be, a minor engaging in sexual activity or depicted in an indecent sexual manner or context."

b. Objectionable material – offences relating to the exhibition, sale and other illegal acts relating to "objectionable films" and "objectionable publications" are covered by the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic). Such material has or would attract a classification of X18+ (restricted) or RC (refused classification) under the *Guidelines for Classification of Films and Computer Games 2005* or National Classification Code scheduled to the *Classification (Publications, Films and Computer Games) Act* 1995 (Cth).

c. Any other material or activity which involves or is in furtherance of a breach of the criminal law.


Category 2: Extreme
This category involves non-criminal use of material that has or would attract a classification of RC under the *Guidelines for Classification of Films and Computer Games 2005* or *National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995* (Cth). This covers any material that:

a. depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should not be classified;

b. describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether or not the person is engaged in sexual activity or not); or

c. promotes, incites or instructs in matters of crime or violence.

Category 3: Critical
This category involves other types of offensive material. This covers any material that:

a. has or would attract a classification of X18+ *under Guidelines for Classification of Films and Computer Games 2005* or National Classification Code scheduled to the Classification

(Publications, Films and Computer Games) Act 1995 (Cth). The material covered by this classification is only available for hire or sale in the ACT and Northern Territory, and covers sexually explicit material that contains real depictions of actual sexual intercourse and other sexual activity between consenting adults;

a. involves racial or religious vilification; c. is unlawfully discriminatory;

b. is defamatory;

c. involves sexual harassment; or

d. brings or has the potential to bring the employee and/or Northside Christian College into disrepute.

Category 4: Excessive personal use during working hours
This category covers personal use which satisfies the following three (3) criteria –

a. it occurs during normal working hours (but excluding the employee's lunch or other official breaks); and

b. it adversely affects, or could reasonably be expected to adversely affect the performance of the employee's duties; and

c. the use is more than insignificant.

Where there is a reasonable belief that illegal activity may have occurred Northside Christian College may report the suspected illegal activity to the police.

**Communication**
These guidelines will be published in part or whole in the College handbooks and in the newsletter, and will be reinforced by College staff on commencement of classes and as required.

**Evaluation**
This policy will be reviewed as part of the College's three-year review cycle.

**Related Policies**
Academic Integrity and Plagiarism Policy

Behaviour Management Policy

Child Safety Policy

Mobile Phone Policy

Privacy Policy

Records Management Policy

Social Media Policy

Student Anti-Harassment and Bullying Policy

## Appendix A: Sample Parent Letter

Dear Parents and Carers,

Northside Christian College has a College wide computer network that supports effective student learning across the College's curriculum. This network also provides student access to the Internet and email.

It is important that you and your child are familiar with the guidelines as stated in the accompanying Information Communication Technology and Internet Acceptable Use Policy.

The aim of the policy document is to:
- Ensure safe and responsible use, and ongoing care of all our ICT resources.

- Safeguard student safety in an online environment.

- Improve student learning outcomes by increasing access to world-wide information.

- Develop skills in appropriate Internet and computer usage.

- Encourage and promote ethical digital citizenship and cyber safety.

The use of your child's account must be in support of, and consistent with, the educational objectives of the College, the College's Behaviour Management Policy and the Information Communication Technology Acceptable Use Policy and Agreement.

Failure to follow these guidelines will result in the loss of privilege to use these facilities.

Although we have established Acceptable Use policies, please be aware that there may be unacceptable material or communications on the Internet that your child can access.

Northside Christian College provides a filtered internet feed and students and teachers will always exercise their duty of care, however, protection against exposure to harmful information on the Internet must depend finally upon responsible use by students.

Please read and discuss the attached policy with your child. Complete and return the signed Agreement to the College Office.

Please contact your child's sub-school Director of Learning should you have any concerns or wish to discuss the matter further.

Yours sincerely


**Principal**

**Appendix B: Student Agreements**



**Computer/Internet Access Agreement**
**PREP – YEAR 2**

The use of Computers and Internet at Northside Christian College is a privilege. They are to be used for educational purposes only.

While I have access to Computers and the Internet, I agree that:

- I can only use the computer when my teacher tells me to use it.

- If I see anything that I think is inappropriate on the computer, I will tell the teacher straight away.

- I will only use nice words when writing on the computer.

- I will only print or use the internet when I am told to do so by the teacher.

- I will only use the apps I have been instructed to use.

- I must log on to the computer using my password and username only. The class teacher will have a copy of this to help me.

- Passwords are not to be shared with other students.

- I will not share personal information about myself to others over the internet.

- Caregivers, teachers and staff at the College are allowed to look at the device at any point to check that students are using it appropriately.

- Any damage to equipment should be reported immediately to the teacher.

- ICT equipment should be treated with care at all times.

I understand that if I break these rules, appropriate actions will be taken. This may include loss of my digital device and Internet access privileges and/or contacting my parents or carers.

**We have read as a family, understood and agree to accept the Computer/Internet Access Agreement.**

Student Name: _____     Year Level: _____

Parent / Carer Signature: _____     Date: ____/____/20___

# Northside
## Christian College

**Computer/Internet Access Agreement**
**YEAR 3 - YEAR 6**

The use of Computers and Internet at Northside Christian College is a privilege. They are to be used for educational purposes only.

While I have access to Computers and the Internet, I agree that:

- I will use them for educational reasons only.

- I will not view or share messages or files that are inappropriate.

- I will not send, receive or download information or software without permission.

- If I come across something that is inappropriate, dangerous or offensive I will clear my screen and tell the teacher straight away.

- I will not share personal information over the internet.

- I will respect the privacy of others.

- I will not use the internet to annoy or offend anyone else.

- I will not give out my password to anyone else or allow someone else to log in and use my account.

- I will not access, alter or delete other students' work or folders.

- I will not claim the work of others as my own.

- I will respect equipment by treating it with care.

- I will not change the settings on school devices.

- I will not access social media such as Facebook, unless given permission.

I understand that if I break these rules, appropriate actions will be taken. This may include loss of my digital device and Internet access privileges and/or contacting my parents or carers.

**We have read as a family, understood and agree to accept the Computer/Internet Access Agreement.**

Student Name: _____     Year Level: _____

Parent / Carer Signature: _____     Date: ____/____/20___

# Northside
## Christian College

**Computer/Internet Access Agreement**

**YEAR 7 – YEAR 9**

The use of ICTs and Internet at Northside Christian College is a privilege. They are to be used for educational purposes only.
While I have access to Computers and the Internet, I agree that:

- I will use them for educational reasons only.

- I will not obtain, view, share or send messages or files containing sexually explicit images, words or coarse language.

- I will not send or obtain any material, information or software or download the same, without permission.

- If I come across something that is illegal, dangerous or offensive, I will clear any offensive pictures or information from my screen and immediately tell the nearest teacher.

- I will not divulge details such as home addresses, phone number, and personal details.

- I will not use the Internet to annoy or offend anyone else.  I will respect the privacy of others.

- I will not give my password to anyone else, or give permission for someone else to use my computer account.

- I will not access other students' work folders or access, alter or delete their files.

- I will not claim the work of others as my own (this is plagiarism).

- I will respect the expensive equipment provided for my use by not disrupting or damaging equipment.

- I will not deliberately change the ICT settings on any equipment or operating environment.

- I understand that it is my responsibility to make backup copies of my work when necessary.

- I will not access Facebook or other social network sites unless given specific permission.

- I recognise that Internet usage is for educational purposes only. Having read this agreement, I agree to abide by the terms and conditions and Computer/Internet rules, as written. I understand that if I break these rules, appropriate action will be taken. This may include loss of my digital device and Internet access privileges and/or contacting my parents or carers.


**We have read as a family, understood and agree to accept Computer/Internet Access Agreement.**

Student Name: _____     Year Level: _____

Student Signature: _____     Date: ____/____/20___

Parent / Carer Signature: _____     Date: ____/____/20___

**SENIOR SCHOOL STUDENT CONTRACT
FOR USE OF PERSONAL TECHNOLOGY AT SCHOOL**

*'Technology' or 'Device' in this document refers to a wide range of hardware, including smart phones, tablets, cameras and laptops.*

*The contents of this contract can be changed at any time. Any changes will be communicated to relevant students.*

At Northside Christian College we recognise the benefits of having access to technology to enhance learning and communication. As such, we allow Senior School students to bring personal devices to school, assuming they abide by the principles listed in this contract. It needs to be understood that Senior School students are not supervised at all times. Students and parents must agree to this contract for the student to be allowed to use personal devices at school.

During class and study periods, technology is to be used only for educational purposes. My device will only be used in class when instructed by the classroom teacher, for the purpose allowed by the teacher. Teachers may still require me to use a physical folder, exercise book etc.

The device is my property and I am fully responsible for its care, maintenance and storage at all times. Any misuse of my device by other students may be my responsibility and financial liability.

Passwords must be kept confidential. I accept full responsibility for any use of my email accounts or similar.

At recess and lunch my device should be used according to acceptable College guidelines. The use of mobile phones during school hours is a privilege, and I will use discretion. Using my phone in front of students who do not have such privileges causes confusion and sets a bad example. If this causes problems I understand the Senior School privileges may be modified or withdrawn.

Any software installed or used at school will meet the ethical and moral standards of the College, and must be age appropriate. Copyright laws should be adhered to. Digital devices may only be used at school on the understanding that teachers may check the contents of the internal memory (hard drive).

I will not capture an image or record sound or video, without the consent of the people being recorded. Content of images, sounds or videos must meet the ethical and moral standards of the College and must never be used to bully or offend anyone, or reflect poorly on the reputation of the College.

Images, sounds or videos should not be shared or uploaded without the permission of everyone in them. Anything that displays the school uniform or logo, is on school grounds or is recorded during school hours cannot be uploaded or shared without the approval of the sub-school Director of Learning.

Bringing personal technology to school is a privilege, and I accept that it may be removed if I fail to keep this contract.

Signed: _____          _____
                    Student's name (Print)                              Signature

Witnessed by parent/s:_____          _____
                                            Parent / Carer 1                              Parent / Carer 2