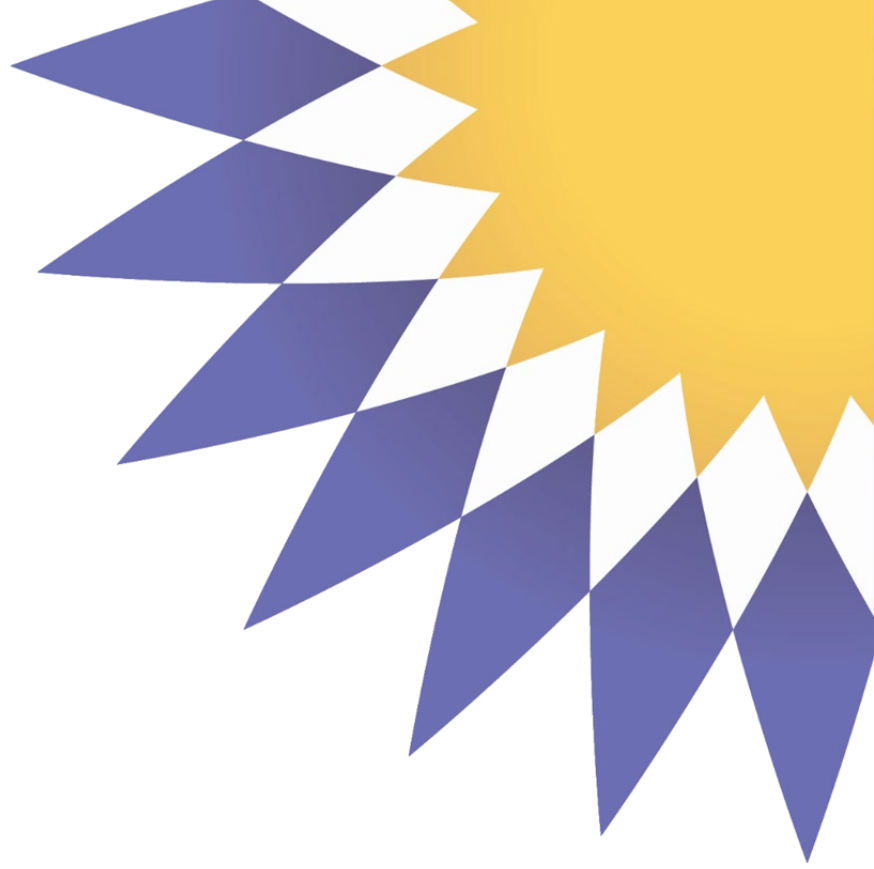




# Tech2Learn

Nambour State College  
P-12 Bring Your Own Device

Charter &  
Application Forms



# Foreword

The Nambour State College Tech2Learn BYO program allows families to provide/purchase a device that will fit the learning style and capabilities of their child attending Nambour State College; allowing them to connect to our departmentally managed networks in a safe and secure environment.

Portable electronic devices such as laptops and iPads are widely used within the school to deliver and enhance student learning. Our curriculum is ever evolving, with Digital literacy being one of the 21st Century skills. Nambour State College offers various ways for students to engage digitally within our college, Tech2Learn programmes encompass both BYO and Hire programs across both Junior and Senior Campuses.

# Table of contents

## Table of Contents

Foreword.....	2
Table of contents.....	3
Tech2Learn BYO Program overview.....	4
Choosing a BYO Device.....	5
BYO Minimum Device Specification .....	5
Device care .....	7
General precautions.....	7
Protecting the screen .....	7
Data security and back-ups .....	7
Acceptable personal device use.....	8
Passwords .....	8
Digital citizenship .....	9
Cybersafety .....	9
Web filtering .....	10
Privacy and confidentiality .....	10
Intellectual property and copyright .....	11
Software.....	11
Monitoring and reporting.....	11
Misuse and breaches of acceptable usage.....	11
Responsibilities of stakeholders involved in the BYOx Device Program:.....	12
What is provided in the Tech2Learn BYO Program.....	15
Acknowledgement.....	16

## Tech2Learn BYO Program overview

Bring Your Own (BYOx) is a new pathway supporting the delivery of 21st century learning. It is a term used to describe a digital device ownership model where students or staff use their personally-owned devices to access the department's information and communication (ICT) network.

Access to the department's ICT network is provided if the child's personally owned device meets the departments minimum operating system and security requirements.

Students are responsible for the security, integrity, insurance and maintenance of their personal devices and their private network accounts.

The BYOx acronym used by the department refers to the teaching and learning environment in Queensland state schools where personally-owned devices are used. The 'x' in BYOx refers to a device of the students' own choice, whether that be a Windows laptop or tablet, or an Apple Laptop or iPad.

We have chosen to support the implementation of a BYOx model because:

- ☀️ Enables the delivery of ICT as an Australian Curriculum general capability.
- ☀️ Fulfil the Education Queensland Core ICT expectations.
- ☀️ Promote student learning outside the classroom,
- ☀️ Investigative learning in new and emerging technologies
- ☀️ Preparing students for an information technology driven world and so much more.

Nambour State College's Tech2Learn BYO program allows students to have the necessary and required technology where and when they need it, using a device which is familiar, suiting their learning style and capabilities.

**Any** device connected to the Internet through Nambour State College's Wireless Network will be subject to Education Queensland's Statewide Departmental web filtering and monitoring. **Students are not permitted to 'hotspot' their devices to avoid using Education Queensland** filtering: i.e., if you have a laptop at school, it should only be connected to the college WIFI. BYOx devices can be Apple Laptop, iPad or Windows Laptops/Tablet devices that are wireless capable (5Ghz).

The College BYOx Device Program supports printing, filtered internet access, and file access & storage through the department's network while at school. Students are responsible for the backup of their data. Students have access to Microsoft OneDrive through their EQ Email Address to facilitate this. It is up to the classroom teacher how these devices are used.

For more information about the Tech2Learn Bring Your Own Device (BYOx) Device Program contact **Andrew Stewart, IT Manager** at [it@namboursc.eq.edu.au](mailto:it@namboursc.eq.edu.au)

Principal

Anthony Green



IT Manager

Andrew Stewart













## Choosing a BYO Device

Before acquiring a device to use at school the parent or caregiver and student should be aware of the school's specification of appropriate device type, operating system requirements and software. These specifications relate to the suitability of the device to enabling class activities, meeting student needs, and promoting safe and secure access to the department's network.



### BYO Minimum Device Specification

Device Type	Microsoft Windows Laptop Apple MacOS Laptop Apple iPad (Only device supported in primary campus) Not Supported: Chromebooks, Android tablets
Screen Size	Laptop - 12" screen or larger (measuring diagonally) iPad – 10.1" screen or larger
Processor	Intel i3/AMD Ryzen 3 -recommended. Apple MacBook/Air/Pro – either Intel or M series-based chip. iPad – 9 <sup>th</sup> Gen or newer (2021) iPad Air – 4 <sup>th</sup> Generation or newer (2020) iPad Pro – 5 <sup>th</sup> Generation or newer (2021)  Not Supported: ARM Qualcomm Snapdragon X processors – found in Microsoft CoPilot+ PC's
RAM	8 GB or higher (16GB Recommended for higher secondary and students interested in CAD or Film/TV/Media)
Hard Drive	256 GB SSD or higher
Operating System	Windows laptop - Windows 11 MacOS Laptop – MacOS 12 Big Sur or newer iPad – iPadOS 16 or newer Not supported- Linux, Android, Windows 7. 8. 8.1, RT, 10S, Chrome OS
Features	Keyboard, headphone port, in-built microphone, webcam  iPads – a keyboard case/cover is highly recommended as this will significantly improve the classroom typing experience.
Battery Life	Minimum of 6 hours +. Please note that it is school policy that devices are fully charged at the beginning of the school day.

Selecting a device is a balance between cost, functionality, weight, and performance. Decide on which considerations are most important to your student and then look for key features to best suit their needs.

Considerations	Features to look for
<p><b>Performance</b></p> <p>Students who are working technically (coding, Graphic or CAD software) or creatively (video editing, illustrating and drawing) will want a device with high performance features.</p>	<ul style="list-style-type: none"> <li> Power and speed: 16GB RAM or higher and i5 core processor or higher</li> <li> Older devices will have a shorter battery life.</li> </ul>
<p><b>Functionality</b></p> <p>Technology rich tasks will require students to use multiple inputs such as audio recordings, videoing, and data logging.</p>	<ul style="list-style-type: none"> <li> Inbuilt microphone</li> <li> Front facing in-built camera.</li> <li> USB port and display port.</li> </ul>
<p><b>Portability</b></p> <p>Consider the portability of the device if your student:</p> <ul style="list-style-type: none"> <li> Uses public transport.</li> <li> Walks long distances</li> </ul>	<ul style="list-style-type: none"> <li> Aim for a lower weight device (around 1.6kg).</li> </ul>
<p><b>Durability</b></p> <p>Accidents happen! Know if your student will likely require a more durable machine.</p>	<ul style="list-style-type: none"> <li> Consider an extended warranty and insurance with follow up support.</li> <li> Solid state hard drives</li> <li> Robust casing and spill-proof keyboards</li> <li> Ruggedized laptops</li> </ul>

## Other BYOD related equipment

-  Headphones with microphone - any headphone that connects with an inbuilt microphone is suitable. Consider cost and student preference.
-  Laptop Case/Sleeve to protect the device. Rigid cases are preferred over soft neoprene/wetsuit material cases as the rigid case provides significantly more protection for the device.

The school's BYOx Device program supports printing, filtered internet access, and file access and storage through the department's network while at school (Internet only for Android devices & iPads). However, the college BYOx Device program does not support additional school technical support or charging of devices at school.

## Device care

The student is responsible for taking care of and securing the device and accessories in accordance with school policy and guidelines. Responsibility for loss or damage of a device at home, in transit or at school belongs to the student. Advice should be sought regarding inclusion in home and contents insurance policy. It is advised that accidental damage and warranty policies are discussed at point of purchase to minimise financial impact and disruption to learning should a device not be operational.

## General precautions

- ☀️ Food or drink should never be placed near the device.
- ☀️ Plugs, cords, and cables should be inserted and removed carefully.
- ☀️ Devices should be carried within their protective case where appropriate.
- ☀️ Carrying devices with the screen open should be avoided.
- ☀️ Ensure the battery is fully charged each day.
- ☀️ Turn the device off before placing it in its bag.

## Protecting the screen

- ☀️ Avoid poking at the screen — even a touch screen only requires a light touch.
- ☀️ Avoid placing anything on the keyboard before closing the lid.
- ☀️ Avoid placing anything in the carry case that could press against the cover.
- ☀️ Only clean the screen with a clean, soft, dry cloth or an anti-static cloth.
- ☀️ Don't clean the screen with a household cleaning product.

## Data security and back-ups

Students must ensure they have a process of backing up data securely. Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost. It is highly recommended that students use the 100GB of web-based storage available in **Microsoft OneDrive**

Microsoft OneDrive allows for Device to Cloud and Cloud to Device synchronising. Every time a file is either created or modified on their device, the OneDrive tool automatically synchronises the files to the cloud. This allows for instances where your device needs to be repaired or replaced, and the hard drive is inaccessible. You can simply sign back into OneDrive on your new device and your files will re-sync automatically.

Students should also be aware that, if any repairs need to be carried out, the service agents may not guarantee the security or retention of the data. For example, the contents of the device may be deleted, and the storage media reformatted.





## Acceptable personal device use

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student(s) access to the internet, based upon the policy contained within the [Acceptable Use of the Department's Information, Communication and Technology \(ICT\) Network and Systems](#)

This policy also forms part of this Student BYOx Device Charter. The acceptable-use conditions apply to the use of the device and internet both on and off the school grounds.

Communication through internet and online communication services must also comply with the department's [Code of School Behaviour](#) and the Responsible Behaviour Plan available on the school website.

While on the school network, students should not:

-  create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place,
-  use unauthorised programs and intentionally download unauthorised software, graphics, or music.
-  intentionally damage or disable computers, computer systems, school, or government networks.
-  use the device for unauthorised commercial activities, political lobbying, online gambling, or any unlawful purpose.




Note: Students' use of internet and online communication services may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

## Passwords

At Nambour State College, your child's network account is secured by a password, along with either their departmental username or email address. Your child's password must be secure enough so that it is not easily guessed by other users.

This password must be kept safe, and not divulged/provided to other individuals as this would be a breach of departmental policy. User accounts and Microsoft 365 logins are not to be shared and are for the sole use of the individual they are provided to.

As part of departmental policy, once a BYO device is enrolled, a secure device password is required to be connected to EQNET Wi-Fi. The policy constraints are as follows:

-  Minimum 8 characters
-  Must contain 3 of the 4 – Upper Case, Lower Case, Number or Symbol e.g. @, #, \$
-  Cannot contain any part of their name.



## Digital citizenship

Students should be conscious creators of the content and behaviours they exhibit online and take active responsibility for building a positive online reputation. They should be conscious of the way they portray themselves, and the way they treat others online.

Students should be mindful that the content and behaviours they have online are easily searchable and accessible. This content may form a permanent online record into the future.

Interactions within digital communities and environments should mirror normal interpersonal expectations and behavioural guidelines, such as when in a class or the broader community.





Parents are requested to ensure that their child understands this responsibility and expectation. The school's Responsible Behaviour Plan also supports students by providing school related expectations, guidelines, and consequences.

## Cybersafety





If a student believes they have received a computer virus, spam (unsolicited email), or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent or caregiver as soon as is possible.

Students must also seek advice if another user seeks personal information, asks to be telephoned, offers gifts by email, or asks to meet a student.

Students must never initiate or knowingly forward emails, or other online content, containing:

-  a message sent to them in confidence.
-  a computer virus or attachment that can damage the recipients' computer.
-  chain letters or hoax emails
-  spam (such as unsolicited advertising).

Students must never send, post, or publish:





-  inappropriate or unlawful content, which is offensive, abusive, or discriminatory.
-  threats, bullying or harassment of another person.
-  sexually explicit or sexually suggestive content or correspondence
-  false or defamatory information about a person or organisation.

Parents, caregivers and students are encouraged to read the department's [Cybersafety and Cyberbullying guide for parents and caregivers](#).

## Web filtering

The internet has become a powerful tool for teaching and learning; however, students need to be careful and vigilant regarding some web content. At all times students, while using ICT facilities and devices, will be required to act in line with the requirements of the Code of School Behaviour) and any specific rules of the school. To help protect students (and staff) from malicious web activity and inappropriate websites, the school operates a comprehensive web filtering system. Any device connected to the internet through the school network will have filtering automatically applied.

The filtering system provides a layer of protection to staff and students against:

-  inappropriate web pages
-  spyware and malware
-  peer-to-peer sessions
-  scams and identity theft.

The web filtering is only active when students are connected to the Education Queensland provided networks (EQQUEST, EQNET and iDET). Outside of these networks, students are not filtered on personal devices, and as such, the school does recommend investigating your own personal solutions for private networks.

Our Mobile Phone Policy – Phones away for the day, further helps to mitigate issues where students may be tempted to hotspot their device to access resources which are blocked by our DoE internet filtering. Please ensure that your child/children are aware, that connecting their personal device to a 3<sup>rd</sup> party internet whilst at school goes against department policy, and appropriate action will be taken.

## Privacy and confidentiality

Students must not use another student or staff member's username or password to access the school network or another student's device, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems.

Additionally, students should not divulge personal information via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school. It is important that students do not publish or disclose the email address of a staff member or student without that person's explicit permission. Students should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

## Intellectual property and copyright

Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. used. It is also important that the student obtain all appropriate permissions before electronically publishing other people's works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the internet or intranet must have the approval of the principal or their delegate and have appropriate copyright clearance.

Copying of software, information, graphics, or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

## Software

Schools may recommend software applications to meet the curriculum needs of particular subjects. Parents/caregivers may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school.

This includes the understanding that software may need to be removed from the device upon the cancellation of student enrolment, transfer, or graduation.

## Monitoring and reporting

Students should be aware that all use of internet and online communication services can be audited and traced to the account of the user.

All material on the device is subject to audit by authorised school staff. If at any stage there is a police request, the school may be required to provide the authorities with access to the device and personal holdings associated with its use.

## Misuse and breaches of acceptable usage

Students should be aware that they are held responsible for their actions while using the internet and online communication services. Students will be held responsible for any breaches caused by other person(s) knowingly using their account to access internet and online communication services.

The school reserves the right to restrict/remove access of personally owned mobile devices to the intranet, internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of personally owned mobile devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.

# Responsibilities of stakeholders involved in the BYOx Device Program:

## School

- ☀️ BYOx Device Program induction - including information on (but not responsible for) connection, care of device at school, workplace health and safety, appropriate digital citizenship and cyber safety
- ☀️ network connection at school
- ☀️ Internet filtering (when connected via the school's computer network).
- ☀️ some technical support (connection to wireless only) - the College policy for staff is "HANDS OFF" student devices
- ☀️ FREE Microsoft Office Student Advantage - visit <http://portal.office.com> and using their department user identification to login.
- ☀️ Adobe Design Software (download at home register at school)
- ☀️ printing facilities
- ☀️ School representative signing of BYOx Device Charter Agreement.

## Student

- ☀️ participation in BYOx Device Program induction
- ☀️ acknowledgement that core purpose of device at school is for educational purposes
- ☀️ care of device
- ☀️ appropriate digital citizenship and online safety (for more details, see <http://www.cybersmart.gov.au/> and <https://www.esafety.gov.au/education-resources/iparent> )
- ☀️ security and password protection - password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students)
- ☀️ some technical support (basic maintenance and operation of privately owned devices)
- ☀️ maintaining a current back-up of data (OneDrive preferred)
- ☀️ charging of device
- ☀️ abiding by intellectual property and copyright laws (including software/media piracy)
- ☀️ internet filtering (when not connected to the school's network)
- ☀️ ensuring personal login account will not be shared with another student, and device will not be shared with another student for any reason.
- ☀️ understanding and signing the BYOx Charter Agreement.

## Parents and caregivers

- ☀️ participation in BYOx program induction
- ☀️ acknowledgement that core purpose of device at school is for educational purposes
- ☀️ internet filtering (when not connected to the school's network)
- ☀️ encourage and support appropriate digital citizenship and cybersafety with students (for more details <http://www.cybersmart.gov.au/>)
- ☀️ some technical support (have in place arrangements for maintenance and repair of privately owned devices)
- ☀️ required software, including sufficient anti-virus software
- ☀️ protective backpack or case for the device
- ☀️ understanding and signing the BYOx Charter Agreement **each year**
- ☀️ adequate warranty and insurance for the device - e.g. accidental damage plan or home and contents insurance that allows for out of home coverage.

## Technical support

	Connection:	Hardware:	Software:
Parents and Caregivers	YES (home-provided internet connection)	YES	YES
Students	YES	YES	YES
School	YES school provided internet connection		YES (Microsoft Office Adobe Design)
Device vendor		YES (see specifics of warranty on purchase)	

The following are examples of responsible use of devices by students:

- ☀ Use devices for:
  - engagement in class work and assignments set by teachers
  - developing appropriate 21<sup>st</sup> Century knowledge, skills, and behaviours
  - authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved by school staff
  - conducting general research for school activities and projects
  - communicating or collaborating with other students, teachers, parents, caregivers or experts as part of assigned school work
  - accessing online references such as dictionaries, encyclopedias, etc.
  - researching and learning through the school's eLearning environment
  - ensuring the device is fully charged before bringing it to school to enable continuity of learning.
- ☀ Be courteous, considerate, and respectful of others when using a device.
- ☀ Switch off and place out of sight the device during classes, where these devices are not being used in a teacher directed activity to enhance learning.
- ☀ Use the personal device for private use before or after school, or during recess and lunch breaks.
- ☀ Seek teacher's approval where they wish to use a mobile device under special circumstances.

## The following are examples of irresponsible use of device by students:

- ☀ using the device in an unlawful manner
- ☀ creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- ☀ disabling settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- ☀ downloading (or using unauthorised software for), distributing or publishing of offensive messages or pictures
- ☀ using obscene, inflammatory, racist, discriminatory or derogatory language
- ☀ using language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
- ☀ insulting, harassing or attacking others or using obscene or abusive language
- ☀ deliberately wasting printing and Internet resources
- ☀ intentionally damaging any devices, accessories, peripherals, printers or network equipment
- ☀ committing plagiarism or violate copyright laws
- ☀ using unsupervised internet chat
- ☀ sending chain letters or spam email (junk mail)
- ☀ accessing private 3G/4G networks during lesson time
- ☀ knowingly downloading viruses or any other programs capable of breaching the department's network security
- ☀ using the device's camera anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- ☀ invading someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- ☀ using the device (including those with Bluetooth functionality) to cheat during exams or assessments
- ☀ take into or use devices at exams or during class assessment unless expressly permitted by school staff.

## What is provided in the Tech2Learn BYO Program

The Tech2Learn BYO program supports personally owned devices in terms of access to:

- ☀ internet
- ☀ support to connect devices to the school network.
- ☀ printing (Windows & Apple devices only)
- ☀ file access and storage (Windows & Apple devices only)
- ☀ Technical advice on issues that may present, and the best course of action to remedy issues.

However, the Tech2Learn BYO program does not support personally owned devices regarding:












- ☀ technical support – the repair of a child's device at school, or where tools must be used to remedy an issue.
- ☀ charging of devices at school
- ☀ security, integrity, insurance, and maintenance
- ☀ private network accounts.
- ☀ Personal data on devices
- ☀ Re-imbursement, financial assistance, repair, or replacement of a device damaged at school by another student.

# Nambour State College Tech2Learn Student BYOx Charter Agreement 2024

Information and Communication Technologies (ICT) includes computers, handheld devices (electronic devices, smartphones, tablets), printers, digital cameras, internet and email facilities, and other associated electronic and mechanical hardware and software. I understand that the use of ICT resources at Brisbane South State Secondary College is a privilege, which involves the acceptance of certain responsibilities.

I understand and agree to the following:

In using ICT resources appropriate for all learning tasks, I am not permitted to:

-  access, copy or distribute any material that is controversial, inappropriate, obscene or offensive;
-  download, install or transfer any software or material that violates copyright, intellectual property or licensing laws;
-  send, transfer or create computer viruses;
-  access the control panel, system configuration, or make any changes to settings, passwords other than those settings my own device
-  directly or indirectly access drives other than those allocated to me;
-  seek access to files or messages intended for, or belonging to, others directly, or indirectly, move, delete or modify any files (other than those in my personal drive);
-  be involved with electronic or physical vandalism, harassment or bullying
-  capture, manipulate or transmit photos of members of staff or students without their prior approval;
-  use any login other than my own;
-  circumvent any security measures on DoE infrastructure
-  use a 3<sup>rd</sup> party internet connection whilst at school e.g. mobile phone hotspot

The College, parents and officials have the right to access and inspect the contents of student files and emails at any time. Random audits of student files will be carried out regularly by IT Network Administrators. Students found to be violating this policy or any law will receive the appropriate consequences and may include referral to appropriate authorities.

I accept that breaching this agreement will result in me losing access to ICT resources temporarily or permanently, depending on the seriousness of the offence. For serious matters, disciplinary action by the Executive team will be taken. I will need to re-negotiate how I use ICTs at school, after my penalty has been served.

## Acknowledgement

By connecting to Nambour State College's Networks, you and your child/children are agreeing to the information and policies, both within this document and referenced in this document. Any breaches will be followed up, in accordance with College processes.





