[School Name]

1. Introduction

To support the delivery of its educational program, the School provides students with access to ICT resources which may include computer/digital devices, internet services at the school grounds, school email accounts and online learning platforms such as cloud based document sharing and classroom tools (**ICT resources**). These ICT resources form part of the learning environment and are supplied to enable students to participate in curriculum activities and are to be used only for that purpose.

This Code sets out the standards expected of students when using ICT resources provided by the school. It explains the measures adopted by the school to support safe and responsible use of ICT resources and identifies the responsibilities of the school, students and parents in managing risks associated with ICT Resource use at the school and at home.

2. Scope

This Code applies to all students enrolled at the school and to all use of ICT resources, devices and the internet where it is provided or managed by the school. It covers:

- use of school supplied devices on site and off site
- use of personally owned devices when connected to school systems
- use of personally owned devices to access school managed cloud platforms or online services whether on site or at home.

This ICT Code of Practice operates in support of the school's Enrolment Agreement and must be followed by students, parents and carers when using ICT resources. If there is any inconsistency, the Enrolment Agreement prevails.

3. Provision of ICT resources and devices by the School

The school recognises that provision of ICT resources is an essential part of a student's modern education. To that end, the School provides the following ICT resources to students:

- devices (computers, laptops, iPads and so on) to support participation in curriculum activities
- access to the internet on school grounds via secure wired and wireless networks for managed devices, or via eduroam for approved personally owned devices.
- through **eduroam**, students may also access the internet at participating eduroam locations. https://eduroam.org/where/
- online educational resources accessible through online platforms such as email, data storage, messaging tools, artificial intelligence and other products and resources hosted online as determined by the school from time to time. These resources may be accessible either on campus at the school or, in many cases, off campus via an internet connection.

4. Technical protections and system controls in place on School devices

The school provides a defined set of measures to support the safe and responsible use of school ICT resources. These measures assist learning, but they do not remove the need for students and parents to act safely and responsibly at all times. The school does not provide any additional supervision, protection or monitoring beyond the measures outlined below or for any non-school devices or ICT resources.

The school has in place the following technical protection measures:

- firewalls and virus protection installed on school owned devices and networks to reduce known security risks
- webpage filtering software installed on school owned devices to block specific website addresses that the school has identified as harmful or inappropriate. The filtering does not analyse or block the content of webpages that remain accessible and does not filter words, messages or other material entered by users on websites, apps or

communication tools. If unsafe websites become known to the School, it will add those to the listed blocked websites on the filtering product.
- logs of activity on school owned devices and school managed platforms may be recorded and retained, and the school may review those logs when required to identify non-compliance with this Code or to protect the integrity and security of school systems
- device management tools used to apply settings, install updates, manage security configurations, and maintain access controls such as screen locks, password requirements, restricted permissions, and other protections required for safe operation of school owned devices.

The school provides educational support to help students use ICT resources safely and responsibly. This support is provided throughout the year as part of regular teaching and learning activities. It includes:
- providing age-appropriate guidance to help students understand safe online behaviour, digital citizenship and the responsible use of ICT resources
- giving general explanations about the limits of technical protections and encouraging students to make safe and sensible decisions when using ICT resources
- offering practical direction and reminders during curriculum activities that involve the use of ICT resources
- providing general supervision of student use of ICT resources during class time as part of normal teaching and learning, noting that such supervision involves general oversight rather than continuous monitoring of individual student activity.

The school provides technical support for school owned devices and school managed platforms. This includes:
- assistance with the operation, basic troubleshooting and maintenance of school owned devices
- software and system maintenance for school owned devices
- guidance with password resets, access problems and similar issues related to school managed systems
- the school may remotely manage, access, lock, disable or reset school owned devices when required to maintain security, recover a lost or stolen device, or support the safe operation of the device.

5. What the school does NOT do

The school does not provide any supervision, technical protection, monitoring or support beyond the measures expressly described in this ICT Code of Practice. The measures the school does provide reduce some risks but do not remove the need for students to act safely and responsibly at all times and for parents to remain involved, supportive and active in supervising and managing students' use of school devices, the internet and ICT resources.

Examples of what the school does not do include:
- supervise or monitor student use of ICT resources when devices are used at home or off the school site
- supervise or monitor the use of private devices, non-school internet services, or accounts not managed by the school
- provide continuous or one to one monitoring of student device use during class time
- observe or view every action taken by a student on a device
- detect harmful or inappropriate content or behaviour in real time
- monitor or access private accounts, personal email services or external platforms that the school does not control
- block all harmful or unsuitable content on the internet
- guarantee that webpage filtering will prevent access to all inappropriate websites
- analyse or filter the content of webpages that remain accessible
- filter or block words, messages or other user generated content entered by students on websites, apps or communication tools
- apply webpage filtering to personal devices or to internet connections not managed by the school
- automatically classify, review or block all newly created or unlisted websites
- guarantee that firewalls, virus protection or filtering tools will prevent all security risks
- guarantee that software updates or security changes will apply immediately or without interruption
- guarantee that devices will operate without faults, errors or technical problems
- provide a standalone or prerequisite course that must be completed before ICT resources may be used
- provide exhaustive or comprehensive online safety training

- supervise or guide students when devices are used outside school hours
- replace the need for parents and carers to supervise their child's use of ICT resources at home
- promise that students will follow the guidance or safety messages they receive at school
- provide technical support for personal devices owned by students or families or home/non-school networks, routers, modems or non-school internet services
- manage, support or secure applications, accounts or platforms that the school does not control.

6. Parent and carer responsibilities

Parents and carers must take a proactive role in supervising, monitoring and educating their child about the safe and responsible use of ICT resources. The support provided by the school during class time must be complemented by active supervision at home. Parents and carers are responsible for their child's use of ICT resources outside the school environment and must encourage open discussion with students about online activity to support the school's monitoring processes and to support the measures the school has in place to reduce risk to students while engaging online.

In addition to the above generally, parents and carers must:

Supervise and monitor ICT use outside the school

- actively supervise their child when a school owned device is used at home or outside the school
- monitor the websites, applications and online services accessed by their child
- set clear expectations for when, where and how the device may be used at home
- remind their child that webpage filtering and technical protections are limited and will not block all harmful or inappropriate content and that if any inappropriate websites are accidentally accessed that the student should immediately report this to the parent
- take steps to restrict or limit access to unsuitable websites or services available on home networks or personal devices.

Support safe and responsible student behaviour

- discuss online safety with their child and reinforce the guidance given at school
- encourage respectful communication and responsible use of all digital platforms
- ensure their child follows the ICT Code of Practice, including rules about communication, content, security and device care
- promote open communication so that their child feels able to raise concerns about online content or behaviour.

Comply with school processes and expectations

- support the school's ICT Code of Practice, its policies and its expectations for safe ICT use
- ensure the school owned device is used only for school related learning activities
- follow school instructions regarding software updates, device management and access requirements (where such instructions are given to you as this would ordinarily be undertaken by the school)
- return the device to the school when requested for servicing, inspection or at the end of the school year.

Understand and act on the limits of school protections

- acknowledge that the school does not supervise home use or monitor private accounts or home networks
- understand that technical protections provided by the school are not comprehensive and may fail
- remain vigilant for unsafe content or misuse that occurs on home networks or private services
- take steps to manage risks in the home environment, including controlling access to other devices or accounts.

7. Student responsibilities and prohibited conduct

Students may use school devices, the internet and all ICT resources but **only for approved school related learning activities** and **in a safe, respectful and lawful manner** that complies with all school rules and values, the ICT Code of Practice and school/teacher instructions and directions as to ICT use.

Examples of appropriate use of school devices, the internet and ICT resources include use to:

- complete assigned class tasks or assignments
- conduct research for class tasks or other school activities

- communicate with teachers or classmates for schoolwork purposes using school approved email or messaging tools
- use school managed systems to store, submit or complete schoolwork
- use digital platforms in a respectful and responsible way that reflects the values and expectations of the school.

Students must not use school devices, the internet or any ICT resource **for any purpose other than what this ICT Code of Practice allows**. Students must not use these resources **in any way that breaks school rules, school policies or the values and expectations of the school**. If a use is not clearly permitted in this Code, it is not allowed. Students must understand that information posted online may be permanent, searchable and shared beyond their control and must act responsibly when contributing to any digital environment. The examples below show specific examples of conduct that is not permitted. Each rule applies at all times.

Students must not use school devices, the internet or any ICT resource to communicate in any way that is rude, unsafe, harmful, illegal, disrespectful or inconsistent with school rules or the values of the school. Examples of this include that students must not:

- send, post or share rude, offensive, threatening or disrespectful messages
- use ICT resources to bully, harass, intimidate, embarrass, defame or target any person
- access, use or join any messaging service, chat room, group call, forum or communication platform that is not expressly approved by the school
- communicate online with any person or artificial intelligence persona other than teachers and students of the school or approved experts for schoolwork
- publish, share or post personal details or images of themselves or others
- arrange to meet or attempt to meet any person they have only interacted with online.

Students must not access, create, share, request, store or encourage others to access any content that is inappropriate, or breaches school rules, values or the law. Examples of this include that students must not:

- access, create, post, share, ask for, store or encourage others to access harmful, unsafe or illegal content including content involving violence, hate speech, adult content, gambling, self harm, drugs, profanity, school violence, pro terror, cyberbullying or child exploitation material or abuse.
- engage in harmful online behaviour including joining chats, groups or platforms that promote violence, bullying, hate speech, self harm, unsafe challenges or any other activity inconsistent with school values or rules or that breaches the law
- visit or engage with any websites or online environments unless they are directly required for the student's current school task and are approved for school use
- copy, download, store or share any material that breaches copyright or other intellectual property rights including music, images, videos or other protected media
- submit work created by another person or by an artificial intelligence tool as their own or otherwise engage in plagiarism.

Students must not alter, interfere with, change, or attempt to change any software, settings, functions, security features or operating features on any device or ICT resource. Examples include that students must not:

- bypass, avoid, evade, work around, disable, interfere with, remove, or attempt in any way to defeat filtering, firewalls, monitoring, or any other security settings or tools installed on any device or ICT resource including through virtual private networks (VPNs), proxies or mobile hotspots
- use another person's name, password or account to access a device or ICT resource or impersonate any person online
- create, use or attempt to use any false or fake online identity, profile or account
- download, install, or use any software, apps or extensions on any device or ICT resource that are not expressly authorised by the school
- attack, damage, or try to compromise any device, system or network
- introduce viruses, malware or harmful software, or attempt to edit, change, alter, or interfere with any system file, source code, operating software, configuration setting, app setting or installed application
- take, share or post screenshots, screen recordings or images of other students, staff or school activities without permission

- hide, delete or try to erase browsing history, activity records or other system logs in order to avoid detection of misuse or non compliance.

Students must not use any artificial intelligence tool, platform or service in a way that is unsafe, inappropriate or inconsistent with school rules or the values of the school. In particular, students must not:

- enter personal, sensitive or confidential information into any AI tool
- create or share personal, sensitive or confidential information or photos about themselves or others using AI tools
- use artificial intelligence tools to generate content that is harmful, unsafe or inconsistent with school rules or values
- use artificial intelligence tools to complete school tasks except where expressly permitted by teachers
- access artificial intelligence tools on devices or accounts that are not approved by the school.

8. Device use, care and financial responsibility

Provision of devices: Students may be provided with school owned devices and accessories to support curriculum activities as part of the all-inclusive curriculum fee. Devices may be (as determined by the School) shared classroom devices, allocated stay-at-school devices or take-home devices. All devices and accessories remain the property of the school and must be returned when requested and at the end of the school year or when a student leaves the school. The school may reset, wipe or reconfigure any device at any time to maintain system integrity and safety.

Responsibilities for care, use and compliance: The safe use and physical care of school owned devices is a shared responsibility between students and parents. The student is responsible for complying with the operational and care requirements set out below, and parents must support compliance and accept financial responsibility for damage or loss that arises from failure to meet these obligations. Students and parents must take all reasonable steps to protect school owned devices and accessories from damage, loss and unauthorised access. Without limitation, this means that Students must:

- bring the device to school fully charged, in working order and ready for learning
- use the device carefully and follow teacher instructions about how, when and where it may be used
- use the supplied protective case or sleeve at all times
- keep passwords private and secure, ensure they are strong and difficult to guess, and change them regularly, at least annually
- take reasonable care to prevent loss, damage or theft
- keep the device with them or stored safely when not in use
- avoid eating or drinking near the device
- immediately report any damage, fault or malfunction to a teacher
- not remove labels or identification markings
- not attempt to repair, modify or clean the device using products not approved by the school
- not interfere with or attempt to bypass any device settings, software, filters or security protections.

Parents must support the student to comply with these requirements and must:

- take responsibility for the care and security of the device when it is not on school grounds
- ensure the student uses the protective case or sleeve correctly
- ensure only approved chargers, cables or accessories are used
- notify the school in writing if damage occurs outside school hours
- report device theft to police immediately, obtain a police report and provide details to the school
- follow school processes for inspection, repair or replacement
- ensure the device is stored safely at home to prevent damage, loss or unauthorised access.

Damage, loss and financial liability: Where a device or accessory is damaged, lost or stolen, the school will assess the cause and determine whether repair or replacement costs are payable. **Parents are financially responsible for damage, loss or theft of a device that the School Principal determines has arisen from:**

- student misuse, carelessness or negligence
- failure to use the supplied protective case or sleeve
- unauthorised modification or interference with the device

- loss or damage occurring outside school hours for any reason
- failure to store the device securely
- loss or damage to accessories such as chargers, adapters or cases, including non return.

Parents may wish to consider separate insurance for any payments they may have to make as a result of the above. Failure to return a device or accessory when requested will be treated as loss for the purpose of cost recovery.

Sale of used devices: Where the school elects to offer used devices for purchase to students/parents, this will be at the school's discretion. Devices will be cleared of data and provided on an as is, where is basis without warranty and may not be the same device previously used by the student.

9. Reporting requirements and incident notification

A strong reporting culture is essential to support the safe and responsible use of ICT resources. Students, parents and carers must promptly report any unsafe, inappropriate or concerning online activity or device use to the School. Early and proactive reporting allows the School to respond and manage risks effectively.

Students, parents and carers must report any matter of concern or breach of this Code of Conduct including any of the following to the school where it occurs in respect of the student or another in using any School device, ICT resource or internet:

- harmful or inappropriate online content accessed on a school owned device
- access to any website that appears unsafe or should be blocked but is not
- messages, communications or behaviour that are rude, unsafe, threatening, harmful or inconsistent with school rules or values
- any online behaviour that makes a parent or student feel unsafe or uncomfortable
- suspected attempts to bypass or interfere with filtering, security settings or other school protections
- any use by any person of ICT resources that appears to breach this ICT Code of Practice
- concern that any technical protections are not operative on a device or that a virus has infected a device
- where a student's password has become known to others or the student is locked out of the device
- damage, faults or technical problems affecting a school owned device
- any concerns about access to school managed platforms including school email, cloud storage or learning tools
- any incident that may place a student at risk of harm when using ICT resources.

Students are encouraged to speak to a trusted teacher or staff member if they feel unsure or worried about what they have seen online or on a device. Reports should be made:

- as soon as possible after an incident or concern arises
- in person, in writing or over the phone to the Principal or any teacher or trusted person at the school (though noting that Counsellors will not typically report the matter on due to confidentiality unless a student permits this)
- with enough detail to allow the school to investigate the concern.

School response to reports and incidents: When a matter is reported, the School will respond in a way that is fair, proportionate and focused on student safety. Depending on the situation, the School may:

- review logs or records stored on school owned devices or school managed platforms to understand what occurred
- examine a device or temporarily restrict its use while inquiries are made into the issue reported
- speak with the student who made the report and any other student involved to clarify the concern
- contact parents or carers where further support or information is required
- take steps to support and protect any student who may be affected
- apply behaviour processes only where a student has engaged in conduct that breaches school rules
- make any referral required under law or school policy.

The school's response will depend on the nature and seriousness of the incident. The Principal has discretion on how incidents are dealt with.

Students may, given the nature of the internet, encounter harmful or inappropriate online behaviour despite the safety measures in place. Where this occurs, the School will provide appropriate support which may include guidance from teachers, wellbeing assistance or other measures designed to help the student manage the impact of the incident. This support is intended to assist students but does not replace the need for parents and carers to actively supervise and guide their child's use of ICT resources outside the school environment.

10. Breach of this Code of Practice

Students must comply with this ICT Code of Practice at all times when using school devices, the internet or any ICT resource. Breaches of this Code may result in consequences applied under the Enrolment Agreement, disciplinary policies and other relevant school policies. The type of consequence will depend on the nature, seriousness and circumstances of the breach.

School response to breaches: Where a breach of this ICT Code of Practice is identified, the School may take one or more of the following actions (as the School Principal determines in their sole discretion is appropriate):

- speak with the student to address the behaviour and reinforce safe and responsible ICT use
- notify parents or carers
- restrict or suspend access to school owned devices or school managed platforms for a period of time
- suspension or expulsion from school
- require the student to complete specified learning activities related to digital safety or responsible use
- confiscate a device for inspection, repair or reset if needed to protect the integrity of the device or school systems
- refer the matter for disciplinary action under the school's behaviour policy or student code of conduct
- require the parents to pay for repairs or replacement to the device
- refer the matter to the principal or senior staff for further action if the breach is significant
- make any referral required by law including notifying authorities
- any other action considered appropriate by the school.

11. Code of Practice Review

This ICT Code of Practice will be reviewed regularly by the school to ensure that it remains current and effective. The school may amend or replace this Code at any time to reflect changes in technology, legal requirements or school processes. Any updated version will take effect once published or otherwise communicated by the school. Students, parents and carers must comply with the most recent version of this ICT Code of Practice.

12. Acknowledgement and agreement

Details of device allocated to student as at date of signing (if any)	• Apple iPad (A18) 128GB Wi-Fi (Silver) / Dell Chromebook 3120 2-in-1 8/64 / HP ProBook 4 G1i Clamshell 16GB/256GB / other: Take home; shared device; stay at school • 3 Year Warrant/3 Year Warranty with Accidental Damage Protection (ADP) / $55 Excess / Nil Excess / Other • STM Dux Case/STM Keyboard Case/Power Adapter/Targus Work-in Dome Case/Targus TANC/Logitech Crayon/other as noted

This ICT Code of Practice operates in support of the school's Enrolment Agreement and must be followed by students, parents and carers when using ICT resources. If there is any inconsistency, the Enrolment Agreement prevails. The Code applies to all students whenever they use school ICT resources, the internet or any school owned device. The Code must be complied with at all times and access to ICT resources is conditional on compliance. The Code applies whether or not this acknowledgment is signed but given its importance, the School requires specific acknowledgement of this Code of Practice.

Parent or Carer Acknowledgment: I acknowledge that I have received, read and understood the school's ICT Code of Practice. I particularly acknowledge that:

- the Code is a school policy that must be complied with by myself and my child under the Enrolment Agreement for my child between myself and the School
- I consent to my child's use of ICT resources and I understand that access to the school's ICT resources and any school owned device is conditional and may be restricted or withdrawn if the Code is breached
- I must support my student to understand and follow the Code including all requirements about care, use and security of school owned devices
- I am solely responsible for supervising my student's device use and online activities outside the school. Any filter on any school device is limited in nature and I must establish my own appropriate supervision arrangements for my child outside the school.
- I am financially liable for repair or replacement costs where damage, loss or misuse occurs in accordance with the Code.

Parent or Carer Signature	
Parent or Carer Name	
Date	
Parent or Carer Signature	
Parent or Carer Name	
Date	

Student Acknowledgment: I acknowledge that I have received and read the School's ICT Code of Practice. I understand and pledge that:

- I must follow the Code whenever I use school devices, the internet or any ICT resource
- I must care for any school owned device in my possession and use it only for school related learning
- I must follow teacher instructions and comply with all rules in the Code
- Access to ICT resources may be restricted or withdrawn if I breach the Code
- Breaches of the Code by me may result in consequences under school discipline policies and the Enrolment Agreement.
- I agree to follow the ICT Code of Practice at all times.

Student Signature	
Student Name	
Date	
Home Group/Class	

Privacy collection statement

CEDR and CEDR Schools are committed to the Australian Privacy Principles contained in the *Privacy Act 1988* (Cth) (**Privacy Act**). CEDR through its Privacy Statement and Information Collection Notice is collecting your information provided by you/the student on this form to insure the appropriate use of the CEDR/school network and devices using the school network. The information will be used and disclosed by authorised CEDR and CEDR school employees for the purposes outlined on this form. Personal information collected on this form may also be used or disclosed to third parties where authorised or required by law. This information will be stored securely. If you wish to access or correct any of the personal information on this form or discuss how it has been dealt with, please contact your CEDR School Principal or Catholic Education – Diocese of Rockhampton Office directly at: *Phone: (07) 4994 8100 Address: 143 West Street, Rockhampton Qld 4700 Australia*