COOLUM BEACH
CHRISTIAN COLLEGE

Acceptable Use of ICT Policy-

STAFF & STUDENTS

Purpose:	The purpose of this policy is to establish clear expectations and guidelines for the responsible, ethical, and secure use of all ICT resources within Coolum Beach Christian College including College-owned ICT resources as well as personal ICT devices when they are used for College-related activities.	
Scope:	This policy applies to all users of ICT at Coolum Beach Christian College including staff, students, volunteers, authorised guests and contractors.	
Status:	In progress	**Supersedes: Feb 2025**
Authorised by:	Board Governing Body	**Date of Authorisation:** Feb 2025
References:	• *Privacy Act 1988 (Cth)* • *Copyright Act 1968 (Cth)* • Australian Privacy Principles • The Australian Student Wellbeing Framework • National Principles for Child Safe Organisations • eSafety Toolkit for Colleges • Queensland Government Department of Education Use of ICT systems procedure *References below are suggestions only. Please amend as appropriate.* • Coolum Beach Christian College Student Code of Conduct • Coolum Beach Christian College Staff Code of Conduct • Coolum Beach Christian College Privacy Policy • Coolum Beach Christian College Copyright Policy • Coolum Beach Christian College Complaints Handling Policy	
Review Date:	Every 2 years	**Next Review Date:** February 2027
Policy Owner:	College Governing Body	

Definitions

- Acceptable use: Use of technology that aligns with the values and purposes of the College and the intent of this policy, complies with relevant laws and regulations, and respects the rights of others.
- AI tools: Computer programs that utilise machine learning algorithms and other advanced techniques to mimic human cognitive abilities like reasoning, pattern recognition, and learning from data. These tools can generate creative content, assist with problem-solving, and automate certain tasks.
- Copyright: Legal protection granted to original creative works.
- Cyberbullying: Repeated online harassment or intimidation targeting an individual.
- Data: Any information stored or transmitted electronically, including personal or sensitive information of students and staff.
- ICT: Information and Communication Technology. Refers to all technology provided by the College used for collecting, storing, processing, transmitting, and communicating information, including computers, networks, software, applications, and internet access, and personal devices used for College-related activities.
- Network resources: Hardware and software infrastructure supporting the College's technology network.
- Personal device: Any electronic device owned by a user that is brought to College or used for College-related activities, such as laptops, phones, tablets, smart watches, etc.
- Plagiarism: Using someone else's work or ideas without conferring appropriate credit.
- College-related activities: Any activity connected to the College, including classes, breaks, assignments, clubs, extracurricular activities, College trips, and online communication of teachers and students.
- User: Any individual authorised to use College ICT, including staff, students, volunteers, authorised guests, and contractors.

ACCEPTABLE USE OF ICT

General Principles

- All ICT use must be responsible, ethical, and legal, respecting the rights and dignity of others.
- ICT should be used to support learning, communication, and collaboration within the College community.
- ICT should be used in a way that maintains a safe and productive learning environment for all.
- To ensure the responsible and safe use of the College's network, Coolum Beach Christian College reserves the right to monitor and maintain appropriate records of network activity (e.g. email, web browsing, file sharing). This monitoring is conducted in alignment with applicable laws to protect the College community and maintain a secure learning environment.

Online Conduct

- Using ICT to engage in any illegal activity, such as hacking, accessing or distributing illegal content, or participating in online scams is strictly prohibited.
- Users must not engage in any online behaviour that is intended to intimidate, humiliate, threaten or harass another person, including sending offensive messages, excluding others from online groups with the intent to ostracise, spreading false or harmful information, or impersonating others.
- Sharing content online that is hateful, discriminatory, promotes violence or illegal activities, or expresses discriminatory views based on protected characteristics such as race, religion, gender, sexual orientation, disability, or any other personal attribute is strictly prohibited.

- Users must not engage in activities that violate community standards of decency and professionalism regarding online content. This includes accessing, viewing, or distributing materials of a sexually suggestive or exploitative nature.

Access and Authorisation

- Access to College technology is granted on a privilege basis and for approved College-related purposes only.
- Limited personal use of College technology may be permitted for staff members during off-duty hours and within the acceptable use parameters outlined in this policy, as long as it doesn't interfere with official duties and incur more than negligible costs.
- Downloading and installing unauthorised software using College technology, including games, gambling software, pirated software, or applications that bypass College security measures or disrupt network performance, is strictly prohibited.
- Users must only access College technology using their own authorised accounts. Sharing of authorised accounts or passwords is strictly prohibited.
- Accessing data or systems that users are not authorised to access, or attempting to bypass security measures to gain unauthorised access is strictly prohibited.
- Users must not share confidential information with unauthorised individuals or organisations.

Data Security and Privacy

- Users should be aware of the risks of online activity and take steps to protect their own data and privacy.
- Users must not collect, store, or share personal information about others without their consent.
- All personal information, including sensitive information, must be handled confidentially and with appropriate security measures to protect against unauthorised access, misuse, or disclosure.
- Users must report potential data breaches or security vulnerabilities in alignment with the Coolum Beach Christian College Privacy Policy and Data Breach Response Plan.

- Coolum Beach Christian College is committed to the responsible and ethical use of AI tools within the College environment. All staff, students,and volunteers are reminded to ensure that any use of AI does not involve the input, processing, or sharing of personal, sensitive, or confidential data. The College prioritizes data privacy and security, and encourages the use of AI in ways that align with our values of integrity, transparency, and ethical digital practice.

- **Online Communication and Behaviour**

- All online communication must be respectful, courteous, and professional.
- Cyberbullying, harassment, and discrimination are strictly prohibited.
- Users must not engage in offensive or illegal online activities.

Content Creation

- Users must respect copyright laws, avoid plagiarism, and not use ICT in any way that impacts on the academic integrity of work produced.
- Using copyrighted materials without permission, such as downloading or sharing music, movies, software, or other copyrighted works without the owner's consent is strictly prohibited.
- Submitting work that is plagiarised is strictly prohibited.

- The College acknowledges the growing role of AI tools in content creation and supports their responsible use. When using AI-generated content, users must ensure that such use aligns with academic and professional standards. Attribution should be provided where appropriate, clearly indicating the involvement of AI tools in the creation process. Users are also responsible for verifying the accuracy, reliability, and appropriateness of AI-generated material before incorporating it into any academic, administrative, or public-facing content. Misuse of AI tools, including uncredited or unchecked content, may be subject to review under relevant College policies.
- Users should be mindful of the potential impact of their digital content on others.

Network and Internet Use

- The College network and internet resources are valuable tools for learning and communication. All users are responsible for using these resources efficiently and prioritising activities that support educational goals.
- Users must be mindful of data download and upload limitations when accessing online content or engaging in network activity and consider the impact their usage might have on others' access and the overall network performance.
- If users' activities require significant data usage, they should consult with relevant staff to explore options and ensure responsible resource allocation.
- Overloading the network with excessive bandwidth usage, downloading large files for personal use during peak hours, or engaging in activities that disrupt others' access to network resources must be avoided.
- Accessing websites or online services that contain harmful content or present security, and privacy concerns is strictly prohibited.
- Using College network resources for personal gain, such as running commercial businesses or engaging in unauthorised online activities is prohibited.

Personal Device Use

- Personal devices may only be used for College purposes with prior permission and under specific guidelines determined by the College from time to time. A consent form may have to be signed prior to being granted permission to use a personal device, containing an agreement to comply with the specific guidelines and this policy.
- Users are responsible for the security and appropriate use of their personal devices on College premises. The College assumes no responsibility for their loss, theft, or damage.
- Personal device use must not disrupt the learning environment or interfere with College activities.
- Personal devices must not be used to access websites or content prohibited on College technology.
- Recording audio or video with personal devices during College-related activities without the express consent of all individuals involved and in contravention to relevant laws and College policies is strictly prohibited.
- Users must not utilise personal email accounts and platforms for College-related communication or storage of College documents.

Use of College Identity

- Coolum Beach Christian College's name, or any images where Coolum Beach Christian College or Coolum Beach Christian College students are identifiable, such as students in uniform, may not be used as content to post online without the express permission of the College. This includes but is not limited to posting images or video footage on social media sites.
- Use of social media must not impact the reputation of Coolum Beach Christian College or any previous/current Coolum Beach Christian College staff or students.

Consequences of Violation

- Coolum Beach Christian College takes violations of this policy seriously. Misuse of ICT may result in a range of consequences, depending on the severity of the offence.
- Possible consequences may include:
    - Discussions: In some cases, violations may be addressed through discussions about acceptable use with the individual(s) involved and, if appropriate, parents or guardians.
    - Access Restrictions: The College may temporarily or permanently revoke a user's access to the network or limit their access to devices to ensure the safety and security of the College's digital environment.
    - Disciplinary Actions: For more serious violations, the College may take disciplinary actions, such as warnings, suspensions, expulsion, or termination of employment, in accordance with established disciplinary procedures.
    - Legal Consequences: Serious violations that involve illegal activities may also have legal consequences, including potential criminal charges.
- Users must report suspected violations of this policy promptly to the Principal, teacher, ICT Department, Student Wellbeing Officer and Head of College.

Resources and Support

- Coolum Beach Christian College will ensure that appropriate information, training, instruction, and supervision is provided to users to enable them to use Coolum Beach Christian College's ICT assets in accordance with this policy.
- For technical assistance, users may contact ithelpdesk@cbcc.qld.edu.au or refer to policy on MyCool.

STUDENTS

Coolum Beach Christian College is committed to educating students to use IT with wisdom and discernment, while also protecting College students from immoral, illegal, or damaging actions by themselves or others, either knowingly or unknowingly. Computer and Internet-related systems at the College, including, but not limited to computer systems, operating systems, software, storage media, copiers, network accounts providing network access, cloud storage, email accounts, WiFi and Internet access are the property of Coolum Beach Christian College. These systems are made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The College's Computer & Internet Acceptable Use Policy has been drawn up to protect all parties - the students at the College.

Each student who obtains an e-mail account or uses the computers made available by Coolum Beach Christian College must understand that he/she is accountable for the policies set forth in this document.

Students who do not use the College's IT resources in accordance with this usage policy will have their network privileges revoked. Any consequent inability to hand in work is entirely the student's responsibility.

General and Educational Use

Students will:

- Use the IT facilities in an ethical and lawful way, in accordance with Australian laws.
- Access must only be made via the authorised account and password, which must not be made available to any other person.
- Not damage, disable, attempt to attack/corrupt, or threaten the integrity of computers, computer systems or networks of Coolum Beach Christian College.
- Only access sites and materials that are appropriate to work in College. Users will recognise materials that are inappropriate and should expect to have their access removed.
- Be responsible for e-mail they send and for contacts made that may result in e-mail being received. All use of internet and online communication services can be audited and traced to the accounts of specific users.
- Use appropriate levels of language and content for messages, email or other media, particularly as e-mail is often forwarded.
- Not post anonymous messages or forward chain letters.
- Not use computer or network services in a way that violates copyrights, patent protections, or license agreements.
- Be permitted to follow legitimate private interests, providing College use is not compromised.

- Not use the College's network to conduct unauthorised commercial activities, personal financial gain, gambling, political purposes, advertising or any unlawful purpose.
- Understand that all data students create on the College systems remains the property of Coolum Beach Christian College.
- For security and network maintenance purposes, understand that authorised staff within Coolum Beach Christian College may monitor student use of equipment, systems, and network traffic at any time.
- Recognise that Coolum Beach Christian College also reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- Understand that the College's IT personnel and teachers are authorised to view any and all files on any device used for the storage or transfer of files (Memory sticks, CDs, MP3 Players, etc) that a student uses with the College's equipment.
- Not use any unauthorised programs and intentionally downloading (from the internet or personal USB drives) unauthorised software, games, graphics, videos, or music that are not associated with learning, are not permitted.
- Use the email address the College provides all students. Use of personal email or chat accounts on the College network is strictly prohibited.
- Not send, receive, or view email or chats of a personal nature using the College's computer systems or network.

Network and Computer Security

Students will:

- Not disable settings for virus protection, monitoring, spam and filtering that have been applied by the College ICT Department.
- Not compromise or attempt to compromise the security of any IT facility belonging to the College or other organisations or individuals, nor exploit or attempt to exploit any security deficiency.
- Keep passwords confidential, and change them when prompted, or when known by another user.
- Use passwords that comply with College Password Security Policy and are not obvious or easily guessed.
- Not allow others to use their personal account.
- Not use another user's personal account.
- Never leave a computer unattended when it is logged on under their account.
- Inform a teacher or an ICT technician if they become aware that an unattended computer is logged on.
- Log off at the end of each session to ensure that nobody else can use their account.
- Never knowingly initiate or forward emails or other messages containing:
    - A message that was sent to them in confidence
    - A computer virus or attachment that is capable of damaging recipients' computers
    - Chain letters and hoax emails
    - Spam (e.g. unsolicited advertising material).

Network Etiquette

Computer systems and networks allow for a free exchange of ideas and information. This exchange serves to enhance learning, teaching, critical thinking and research. While we highly encourage the free exchange of ideas and information, we also require students to be respectful and civil.

Students will:

- Cooperate with other users of the IT facilities to ensure fair and equitable access to the facilities.
- Use appropriate language. Do not swear, use vulgarities or any other inappropriate language or obscenities.
- Be polite and treat all persons with respect and dignity. Do not harass or bully anyone based on gender, race, disability, or social status.

Never send or publish:

- Unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
- Communications or advocacy directed to incite or produce lawless action.
- Anonymous or repeated messages or communications designed to threaten, annoy, abuse, or torment any person.
- Sexually explicit or sexually suggestive material or correspondence.
- False or defamatory information about a person or organisation.
- Communications otherwise designed to disrupt the educational environment.

Privacy and Confidentiality

Technology should not be used in a manner that infringes upon an individual's right to privacy. The following restrictions are meant to protect students' privacy, as well as the privacy of others.

Students will:

- Never read, copy, change or delete another student's work.
- Never read, forward, delete, or otherwise tamper with another user's e-mails.
- Never publish or disclose the email address of a staff member or student without that person's express permission.
- Never interfere with another student's electronic identity, as per our Digital Citizenship values.
- Not reveal personal information including their names, addresses, telephone numbers, parents' details, photographs, videos, or the name and location of the College without their parents' or teacher's permission.
- Seek advice from a teacher if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.

Academic Fraud, Intellectual Property, & Copyright

Students will:

- Never use the College IT facilities to sell or purchase assignments, or to offer to write assignments or to request other students to complete another student's assignments.
- Never plagiarise information from any source and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- Ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.
- Ensure any material published on the internet or intranet has the approval of the Principal or their delegate and has appropriate copyright clearance.

Use of Collaborative Online Websites

The following rules govern students' use of all online collaborative or social networking systems used by the College:

- Normal classroom rules apply to internet-based collaborative space used by a student in the course of their study at the College, as the collaborative space is an extension of the class and the College. Students are representing the College on the internet. The College's Christian belief system and standard of behaviour applies to all web- based College activities.
- Upon establishment of a blog, wiki, social networking site, social bookmarking, online file-sharing environment, or other collaborative site, all posts and comments must be moderated by the teacher in charge before publication.
- The teacher is to be the only administrator of such collaborative sites. Student editorial rights are not to exceed the status of editor. Students are not to change or attempt to change any password. Students may not delete a teacher's rights, nor may they alter or delete the site account(s).
- There should be no direct connection of other subscribers (persons external to the College) of the site to students without the permission of parents/guardians.
- The Administrator of the site has the right to 'not approve' comments from subscribers, and is not obligated to supply a reason for not approving a comment.
- Where students set their own usernames, students must ensure that usernames are of an appropriate nature.
- Students are not to link their personal social networking sites or profiles to those used by the College, or on the College systems.
- It is intended that at the end of each year, collaborative web-based tools will be 'locked down', allowing students to read material but not upload further comments. The sites may be re-opened the following year, with parental permission, if the project is continuing.
- Students who transfer out of the College or a class will lose permissions to alter material created in collaborative online environment relating to their being a student of the College or one of its classes.

- Students are not to use their full names on collaborative web-based sites and tools used by the College. Students are to refer to themselves by first name and initial only, if necessary.
- Students may not give the home address, personal email, phone numbers, or other personal information belonging to another student or to any other person on any College web-based sites.
- The work on collaborative web-based sites done in a College context must be of an educational nature. The use of the College computers, network, or other equipment for web-based activities that are of a personal nature are prohibited.
- Debating and discussing of issues is acceptable in a collaborative, online environment. Students must always ensure that the tone of any submissions they make show respect to all other persons and their opinions.

YouTube

The Terms of Service for the use of YouTube set by Google include that all users of the service affirm that they are either:

- at least 18 years of age,
- an emancipated minor; or,
- are at least 13 years of age and have consent from a parent or legal guardian to use YouTube.

Google recommends that users under the age of 13 not use the service as it is not considered appropriate for children under the age of 13. Google requires that all Colleges using G Suite for Education follow these guidelines and receive permission from a parent or legal guardian for students under the age of 18 to use YouTube. Therefore, agreement with this Computer and Internet Acceptable Use Policy includes providing permission for students to access YouTube at the College and as part of their classes.

Primary students will only be given access to a heavily filtered and moderated version of YouTube at the College, and Secondary students will be provided a somewhat restricted access to YouTube (with keyword filtering and content moderation).

Personal Responsibility

Each student is responsible for:

- Reporting unauthorized use of their account.
- Reporting any breech of system security.
- Reporting any Internet site accessed that is considered inappropriate.
- Reporting any faults or problems to their teacher, the ICT. Faults may include suspected software failures, hardware failures, or broken or damaged equipment.
- Informing their supervising teacher or the ICT if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.

- Being familiar with, and adhering to, College eSmart values.
- Frequently saving and making back-up copies of their work to protect against loss.
- Clearly labelling works and opinions as his/her own before they are widely distributed.
- At the end of their time here at the College, copying to their own personal storage device (e.g. USB drive) any of their own files they wish to retain. The College suspends a student's account, including email and cloud storage, upon departure to reclaim available licences for software.

Misuse/Hacking of IT Facilities

- Vandalism - Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to damage or destroy any computing, printing, networking, or other IT equipment owned or leased by the College.
- Unauthorised Software - Users are forbidden from attempting to install their own software or software that they have downloaded from the internet or obtained from another source. Attempts to install unauthorised software may results in all cancellation of network privileges.
- Unauthorised Access to Accounts - Users are expressly forbidden unauthorised access to accounts, data or files on College IT facilities, or on IT facilities belonging to other organisations.
- Peer-to-Peer File-sharing Programs - installation or use of peer-to-peer file-sharing programs such as BitTorrent, etc is not permitted on any device connected to the College network.
- Games - Game playing is not allowed on the College IT facilities, except as a formal component of a College class or through a faculty sponsored event.
- Inappropriate Sites or Files - Users are not permitted to utilize the College's IT facilities to access inappropriate site or contents including, but not limited to, pornographic content; or to create, store or distribute pornographic or other inappropriate content or files. There will be no acceptable defence for a violation of this policy.
- Coolum Beach Christian College Logo and Name - Users are not permitted to use the College's name, logo, or other likeness on their personal web pages, email, or other messaging facilities.

The College reserves the right to withdraw a service or withdraw access to the College network, even for student owned computers, if there is evidence of any misuse or hacking of the College's IT facilities.

Mobile Phones

Mobile phones, Smart Watches, MP3 players and all other similar digital devices have become an acceptable technological accessory for people of all ages to use to their own advantage. As in the wider society, so too is this the case increasingly in Colleges. **The College is a mobile free environment for students, therefore mobile phones are not to be brought to College.**

Smart watches must be switched to College mode (i.e. no sending or receiving of messages and images, no internet access, no access to games or music on the watch.

Whilst the College has taken this position, there will be times where parents need their child to be in possession of a phone for important contact requirements before and after College, or in medical cases, throughout the College day. There may also be times where a teacher requires students to bring their phone for a specific class related activity. In these situations, **permission will be given on a case-by-case basis for students to bring their phone to College.**

Students will:

- Not bring mobile phones to College unless given permission to do so by the College.
  In instances where mobile phones may be permitted at College the following must be adhered to:
- Not use mobile phones to bully, harass or threaten other students at the College.
- Not to use in-phone cameras to photograph or film other individuals without their consent. This includes staff and students at the College.
- Not use in-phone or digital cameras in toilets, changing rooms, bathrooms or in any situation that may cause embarrassment or discomfort for other individuals, students, staff or visitors to the College.
- Switch off mobile phones or other digital devices during all tests and examinations.
- Ensure mobile phones or other digital devices are stored in a secure place and that students are fully responsible for them, including guarding against loss, damage, or inappropriate use. Storage of these devices in student bags is not advisable.
- Not wear or use headphones or earphones during College hours unless a teacher has given permission to do so during class.
- Realise that mobile phones or portable digital devices that are brought onto the College grounds are used at the owner's risk. The College does not accept liability in the event of the loss, theft or damage of any device.
- Not publish photos or material online, including social networking sites, without that individual's consent. This includes staff and students at the College.

Investigation

When the College becomes aware that a student may have accessed websites and/or files that are inappropriate, the appropriate Head of College will be notified. The Head of College will investigate the misuse, and utilise their skills in behaviour management and student wellbeing to educate and, if necessary, discipline the students.

Disclaimer

While every effort is made to maintain the reliability of the College network and associated systems, Coolum Beach Christian College makes no guarantees the network

will be without fault. The College accepts no responsibility and makes no warranties of any kind, whether expressed or implied, for:

- Loss or damage or consequential loss or damage, arising from the use of its IT facilities for academic or personal purposes whether from delays, non-deliveries, mis- deliveries, or service interruptions caused by its own negligence or student errors or omissions.

- Loss of data or interference with files or email arising from its efforts to maintain the IT facilities.
- The accuracy, quality, or trustworthiness of any information obtained via the Internet over the College network

STUDENT SAMPLE OF AGREEMENT (sent electronically to Parents and Caregivers)

All students will have access to our College Network and the Internet and should sign a copy of this Statement and return it to the College for approval.
I, Parent's/Guardian's Name:

_____

(PLEASE PRINT)

Permit Student's Name:

_____

(PLEASE PRINT)

Year Level: _____

to participate in the use of technology at CBCC and in accordance with the College policy and procedures

I understand and acknowledge my responsibilities and those of Coolum Beach Christian College by signing this.

Student's Signature:
_____ Date:
/ /

Parent's/Guardian's Signature:

_____

Date: / /

STAFF

All employees at Coolum Beach Christian College are responsible for utilising ICT services to enhance teaching, learning and for business operations. Coolum Beach Christian College expects this technology to be utilised to its full capacity to provide the most valuable learning and teaching environment to the benefit of all.

Coolum Beach Christian College also expects employees to demonstrate acceptable use via safe, lawful, and ethical behaviour whenever using ICT services.

This Policy applies to the management of all types of ICT services, as defined in the "Definitions" section below. This Policy also applies on the College premises, as well as during College activities, such as excursions, camps, and extra-curricular activities whenever Coolum Beach Christian College ICT services are utilised. It also applies to all CBCC owned equipment and services e.g., internet activity, at all times irrespective of physical location.

Coolum Beach Christian College reserves the right to restrict employee access to ICT services if access and usage requirements are not met or are breached.

Employees should also note that breaches of this Policy may result in disciplinary action or criminal proceedings.

Definitions

College provided and personal devices includes all types of mobile and smart phones, laptops, tablets, cameras and video recorders, music devices, USBs, eBook readers, other palm and handheld devices and other equipment, as determined by the College, and owned by the College and employees.

Acceptable use: Use of technology that aligns with the values and purposes of the College and the intent of this policy, complies with relevant laws and regulations, and respects the rights of others.

- AI tools: Computer programs that utilise machine learning algorithms and other advanced techniques to mimic human cognitive abilities like reasoning, pattern recognition, and learning from data. These tools can generate creative content, assist with problem-solving, and automate certain tasks.
- Copyright: Legal protection granted to original creative works.
- Cyberbullying: Repeated online harassment or intimidation targeting an individual.
- Data: Any information stored or transmitted electronically, including personal or sensitive information of students and staff.

- ICT: Information and Communication Technology. Refers to all technology provided by the College used for collecting, storing, processing, transmitting, and communicating information, including computers, networks, software, applications, and internet access, and personal devices used for College-related activities.
- Network resources: Hardware and software infrastructure supporting the College's technology network.
- Personal device: Any electronic device owned by a user that is brought to College or used for College-related activities, such as laptops, phones, tablets, smart watches, etc.
- Plagiarism: Using someone else's work or ideas without conferring appropriate credit.
- College-related activities: Any activity connected to the College, including classes, breaks, assignments, clubs, extracurricular activities, College trips, and online communication of teachers and students.
- User: Any individual authorised to use College ICT, including staff, students, volunteers, authorised guests, and contractors.

General Principles

- All ICT use must be responsible, ethical, and legal, respecting the rights and dignity of others.
- ICT should be used to support learning, communication, and collaboration within the College community.
- ICT should be used in a way that maintains a safe and productive learning environment for all.

To ensure the responsible and safe use of the College's network, CBCC reserves the right to monitor and maintain appropriate records of network activity (e.g. email, web browsing, file sharing). This monitoring is conducted in alignment with applicable laws to protect the College community and maintain a secure learning environment.

Responsibilities

College Responsibilities

Coolum Beach Christian College acknowledges its responsibility to:

- Develop and implement this Policy to ensure the full utilisation of ICT services as essential teaching, learning and business tools within acceptable use parameters.
- Communicate this Policy to employees, ensuring that it is understood and acknowledged by employees.
- Implement risk management measures to reduce the likelihood of network access to harmful information:
- including monitoring/auditing internet and email activities,
- keeping appropriate records,
- monitoring and reporting on any issues related to inappropriate ICT services, and

- any accidental access to inappropriate internet sites or where access to a site leads to inappropriate content must be reported by the worker to the Head of ICT immediately.
- Encourage employees to contribute to a healthy College culture.

Staff Responsibilities

Employees are responsible for ensuring:

- Acceptable use procedures are followed for the business systems and devices they use.
- Other email systems (e.g. personal email services) and social media are not used for the distribution of work-related information.
- Individual use of the College internet and email can survive public scrutiny and/or disclosure.
- Emails that form records are saved into an authorised recordkeeping system and should not be uploaded to personal cloud storage.
- Students' personal information is not emailed outside the College's network, is used for
- legitimate purposes and in accordance with privacy policies.
- Their limited personal use of ICT systems and devices does not violate any other College policy.
- Incidents such as receiving hateful, offensive, or illegal material are reported.
- Unsolicited email 'spam' is reported to the Head of ICT.

Employees can use ICT for personal activities within the following parameters:

- It is infrequent and brief.
- It does not interfere with the normal running of the College.
- It does not breach any law, regulation, standard, code or other policy or related procedure.
- It does not impede that employee's or any other employee's ability to do their job.
- It occurs during off-duty hours (including before and after work and during breaks)
- It is not for private commercial purposes or otherwise for the purpose of generating private income for the employee or another individual.
- It is subject to the same monitoring practices as employment related use and may be subject to disclosure under the Right to Information Act 2009 (Qld) and Information Privacy Act 2009 (Qld).

  Inappropriate use of ICT facilities and devices may result in restricted access to ICT facilities, disciplinary action (including dismissal) and/or action by the police. Under the acceptable use policy:

- Employees found to be intentionally accessing, downloading, storing, or distributing pornography using College ICT facilities and devices will be dismissed.

- Employees may be disciplined or dismissed for the misuse of the internet, email or social media in respect of material that is offensive or unlawful.
- A pattern of behaviour (for example, repeated use) is a factor in determining disciplinary measures (including dismissal).
- Some actions by an employee may constitute a crime, under the Criminal Code Act 1988 (Qld) or be viewed as serious misconduct, and could lead to suspension, exclusion, loss of employment and/or prosecution.

Employees will:

- Exercise a duty of care regarding student access to and use of the College's ICT facilities.
- Provide guidance for use of their ICT facilities and devices within the classroom, including ensuring students understand and follow the College's policies and guidelines.
- Uphold the College's Policy on this issue via their own safe, lawful, and ethical use of ICT services.
- Take reasonable steps to prevent and appropriately respond to any instances of inappropriate use by students of ICT services.
- Immediately advise the Principal if they receive a message that is inappropriate or makes them feel uncomfortable.
- Be aware of occupational health and safety issues when using computers and other learning devices.
- Obtain prior approval form the Principal (in writing) to use personal devices to take photos of students. If a College owned device is used for photos, prior approval is required.

Online Conduct

- Using ICT to engage in any illegal activity, such as hacking, accessing or distributing illegal content, or participating in online scams is strictly prohibited.
- Users must not engage in any online behaviour that is intended to intimidate, humiliate, threaten or harass another person, including sending offensive messages, excluding others from online groups with the intent to ostracise, spreading false or harmful information, or impersonating others.
- Sharing content online that is hateful, discriminatory, promotes violence or illegal activities, or expresses discriminatory views based on protected characteristics such as race, religion, gender, sexual orientation, disability, or any other personal attribute is strictly prohibited.

- Users must not engage in activities that violate community standards of decency and professionalism regarding online content. This includes accessing, viewing, or distributing materials of a sexually suggestive or exploitative nature.

Backup procedures information and system backup

- Procedures and archiving are in place to ensure that in the event of a loss, restoration can take place within acceptable parameters to ensure business continuity.
- Employees must not store the only copy of important information on storage media that is not regularly backed up. This includes storing information on local hard drives, desktops, or removable media.
- College information must not be taken offsite in the form of a portable memory device to mitigate against contravention of data privacy.

Administrators of ICT business systems and software applications must:

- Regularly review and identify users, their roles, registration identification requirements and level of information access in accordance with their level of responsibility.
- Disable access or modify when their requirements change, such as a change in job role, if a person leaves permanently, or is on leave for a prolonged period.
- Restrict access only to information that is necessary to undertake their duties; or they are continually supervised by another worker who has the appropriate authority to access the system.
- Regularly educate employees on adherence to password and security requirements of the ICT business system in use and the potential ramifications of breaching this, i.e., disciplinary action or criminal proceedings.

The Head of ICT must:

- Ensure appropriate security mechanisms are in place to protect data from unauthorised access or modification and accidental loss or corruption
- Identify and implement access restrictions and segregation/isolation of systems into all infrastructures, business and user developed applications
- Manage directories of users including allocating and resetting passwords, user access, security and data backup, and storage of directories
- Establish controls and processes for user registration, authentication management, access rights (including changes to access rights) and privileges.

Access and Authorisation

- Access to CBCC technology is granted on a privilege basis and for approved CBCC - related purposes only.
- Limited personal use of CBCC technology may be permitted for staff members during off-duty hours and within the acceptable use parameters outlined in this policy, as long as it doesn't interfere with official duties and incur more than negligible costs.
- Downloading and installing unauthorised software using CBCC technology, including games, gambling software, pirated software, or applications that bypass CBCC security measures or disrupt network performance, is strictly prohibited.
- Users must only access CBCC technology using their own authorised accounts. Sharing of authorised accounts or passwords is strictly prohibited.
- Accessing data or systems that users are not authorised to access, or attempting to bypass security measures to gain unauthorised access is strictly prohibited.
- Users must not share confidential information with unauthorised individuals or organisations.

Data Security and Privacy

- Users should be aware of the risks of online activity and take steps to protect their own data and privacy.
- Users must not collect, store, or share personal information about others without their consent.
- All personal information, including sensitive information, must be handled confidentially and with appropriate security measures to protect against unauthorised access, misuse, or disclosure.
- Users must report potential data breaches or security vulnerabilities in alignment with the CBCC Privacy Policy and Data Breach Response Plan.

Online Communication and Behaviour

- All online communication must be respectful, courteous, and professional.
- Cyberbullying, harassment, and discrimination are strictly prohibited.
- Users must not engage in offensive or illegal online activities.

Content Creation

- Users must respect copyright laws, avoid plagiarism, and not use ICT in any way that impacts on the academic integrity of work produced.
- Using copyrighted materials without permission, such as downloading or sharing music, movies, software, or other copyrighted works without the owner's consent is strictly prohibited.
- Submitting work that is plagiarised is strictly prohibited.

- AI – Whilst the landscape around AI is changing quickly, it is the position of CBCC to coach students to be responsible digital citizens.
- In practice students will be taught to use AI appropriately for enhancing their learning. Students may not use AI for assessments or avoiding the learning expected by the teacher.
- Users should be mindful of the potential impact of their digital content on others.

Network and Internet Use

- The CBCC network and internet resources are valuable tools for learning and communication. All users are responsible for using these resources efficiently and prioritising activities that support educational goals.
- Users must be mindful of data download and upload limitations when accessing online content or engaging in network activity, and consider the impact their usage might have on others' access and the overall network performance.
- If users' activities require significant data usage, they should consult with relevant staff to explore options and ensure responsible resource allocation.
- Overloading the network with excessive bandwidth usage, downloading large files for personal use during peak hours, or engaging in activities that disrupt others' access to network resources must be avoided.
- Accessing websites or online services that contain harmful content or present security and privacy concerns is strictly prohibited.
- Using CBCC network resources for personal gain, such as running commercial businesses or engaging in unauthorised online activities is prohibited.

Personal Device Use

- Personal devices may only be used for CBCC purposes with prior permission and under specific guidelines determined by the CBCC from time to time. A consent form may have to be signed prior to being granted permission to use a personal device, containing an agreement to comply with the specific guidelines and this policy.
- Users are responsible for the security and appropriate use of their personal devices on CBCC premises. The CBCC assumes no responsibility for their loss, theft, or damage.
- Personal device use must not disrupt the learning environment or interfere with CBCC activities.
- Personal devices must not be used to access websites or content prohibited on CBCC technology.
- Recording audio or video with personal devices during CBCC -related activities without the express consent of all individuals involved and in contravention to relevant laws and CBCC policies is strictly prohibited.
- Users must not utilise personal email accounts and platforms for CBCC -related communication or storage of CBCC documents.

Software Licence Management

The College implements and manages the purchase, installation, maintenance and retirement of software and licences. To ensure compliance employees must:

- Comply with the software's terms and conditions of use.
- Not breach any copyright or anti-piracy laws.
- Not copy any unauthorised software (including any personally owned software) to their device.
- Notify a supervisor, manager or above if they become aware of unlicensed or unauthorised software.

ICT Security

- Use of the College's ICT network is secured with a username and password. The password must be strong enough so as not to be guessed by other users and is to be kept private by the worker and not divulged to other individuals
- Employees cannot use another student or worker's username or password to access the College network, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems
- If a worker suspects their username/password is being used by another person, it is their responsibility to inform their line manager or Head of ICT and arrange for their password to be changed immediately. Failure to do so will mean the worker may be held liable for what happens within their account.
- Employees need to understand that copying of software, information, graphics, or other data files may violate copyright laws and without warning may be subject to prosecution from agencies that enforce such copyrights.

Responsibilities – Use of Personal Device By Employees

For safety reasons, a phone is permitted to be in reach so that it can be used to manage a critical incident (e.g. to call admin or emergency services) if a phone is out of range

Please avoid using a personal phone to call parents or other key stakeholders. Please use the College phones (e.g. landline or admin/excursion mobile phone), when possible.

Behaviour

It is unacceptable for employees while at College to:

- Use the ICT facilities and devices (including personal devices) in an unlawful manner.
- Download, distribute or publish offensive messages or pictures.
- Install, copy, share, or download unauthorised software/applications.
- Use obscene, inflammatory, racist, discriminatory, or derogatory language.

- Use language and/or threats of violence that may amount to bullying and/or harassment, or even stalking (including cyberbullying).
- Insult, harass or attack others or use obscene or abusive language.
- Damage computers, printers, or network equipment.
- Commit plagiarism or violate copyright laws.Knowingly download viruses or any other programs capable of breaching the network security.
- Use in-device cameras anywhere a normal camera would be considered inappropriate.
- Invade someone's privacy by filming/recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material.
- Undertake hacking or intention to breach College security, copyright breaches, pirating and loading of unauthorized discs, and other storage devices onto the College system. This is a breach of this policy and will result in action being taken.
- Sites for personal use such as personal web spaces, chats/forums and other personal sites are not to be accessed at College.
- Employees must be aware electronic communication, including College phone system, is not guaranteed to be private and all email should be considered a public document. System administrators of the network have access to all mail sent and received and automatic filtering of emails and internet use occurs.
- Filtering of websites does occur but any accidental access to inappropriate internet sites must be reported immediately or if employees receive inappropriate emails from anyone.

The College Reserves the Right To:

- Monitor and record all usage of its computer networks, including internet services by regularly filtering the network for inappropriate/non-education files and if found, delete these automatically. This includes worker emails.
- Restrict access to internet and intranet services, where necessary.
- Cull/archive worker files to remove unnecessary files and/or to regain storage space.
- Take disciplinary action when breaches of expected behaviour occur.

The College monitors and reports on intranet, internet and network usage and inspects email messages sent or received by anyone using the College's ICT facilities and devices to:

- Identify inappropriate use.
- Protect system security.
- Maintain system performance.
- Protect the rights and property of the College.

Use of CBCC Identity

CBCC name, or any images where CBCC or CBCC students are identifiable, such as students in uniform, may not be used as content to post online without the express permission of the CBCC . This includes but is not limited to posting images or video footage on social media sites.

- Use of social media must not impact the reputation of CBCC, or any previous/current CBCC staff or students.

Consequences of Violation

CBCC takes violations of this policy seriously. Misuse of ICT may result in a range of consequences, depending on the severity of the offence.

Possible consequences may include:

- Discussions: In some cases, violations may be addressed through discussions about acceptable use with the individual(s) involved and, if appropriate, parents or guardians.
- Access Restrictions: CBCC may temporarily or permanently revoke a user's access to the network or limit their access to devices to ensure the safety and security of the CBCC 's digital environment.
- Disciplinary Actions: For more serious violations, the CBCC may take disciplinary actions, such as warnings, suspensions, expulsion, or termination of employment, in accordance with established disciplinary procedures.
- Legal Consequences: Serious violations that involve illegal activities may also have legal consequences, including potential criminal charges.
- Users must report suspected violations of this policy promptly to ICT Team or Principal.

Resources and Support

CBCC will ensure that appropriate information, training, instruction, and supervision is provided to users to enable them to use CBCC ICT assets in accordance with this policy.

For technical assistance, users may contact IT Helpdesk@cbcc.qld.edu.au

Implementation

Awareness

- Regularly raise awareness of acceptable ICT usage, through the development and implementation of an acceptable use of ICT services policy, which is available on the shared drive, highlighted in the worker handbook and included as part of the induction process.

Training

- Regularly educate and train employees

Record keeping, monitoring, reporting

- Keep appropriate records and logs of ICT usage and monitor and report on any issues related to ICT services

Culture

- Encourage employees to contribute to a healthy College culture.

Compliance and Monitoring

All employees are responsible for ensuring that ICT equipment and devices are used only within the parameters of acceptable use. Any employees who do not use ICT equipment and devices in an acceptable manner will be reported to

the Principal.

Sample of Staff Agreement

COOLUM BEACH CHRISTIAN COLLEGE ACCEPTABLE USE STAFF POLICY

I, (PLEASE PRINT)

Agree to participate in the use of technology at Coolum Beach Christian College and in accordance

with the College's Acceptable Use Policy.

I understand and acknowledge my responsibilities and those of the College by signing this.

Staff Member's Signature:

Date: