Student Acceptable Use Policy: Digital, Online and Artificial Intelligence Services

November 2026

CATHOLIC SCHOOLS BROKEN BAY
Caroline Chisholm Centre Building 2, 423 Pennant Hills Road, Pennant Hills, NSW 2120 | PO Box 4509 Thornleigh NSW 2120
02 9847 0000 | csbb.catholic.edu.au | csbb@dbb.org.au

Rationale

The Student Acceptable Use Policy (**Policy**) sets out Catholic Schools Broken Bay's (**CSBB**) position on students' appropriate use and management of digital systems, online services and artificial intelligence (AI) in accordance with legal and system requirements.

Audience

This policy applies to all students and parent/carers of students.

Definitions

Digital services: hardware, software, applications, databases, networks, and cloud-based platforms that collect, store, process, manage, or transmit information. Digital services include both connected and non-connected technologies.

Online services: require or utilise an internet or network connection to provide services, enable communication, share information, or facilitate collaboration between users, devices, or external services.

Digital communications: any messages, information, data, images, audio, video, or other content that are created, sent, received, stored, shared, or accessed using digital or online services.

Cyber bullying: the use of digital or online services to bully, harass, threaten, embarrass, exclude, intimidate, impersonate or target another person.

Artificial Intelligence (AI): the ability of a computer system to perform tasks that would normally require human intelligence, such as learning, reasoning, and making decisions.

Generative AI (GenAI): field within AI that creates new content such as text, images, voice, video, and code by learning from data patterns.

Filtering: the use of technical controls to limit, block or allow access to websites, online content, applications, services or network activity in order to support safe, appropriate and educational use of CSBB digital and online services.

Monitoring: the authorised review, logging or analysis of activity, communications, access records, system use or security events on CSBB digital systems, networks and online services to support safety, wellbeing, cyber security, system performance, compliance and investigation of suspected misuse.

Policy

Digital Devices

Students may be provided with or authorised to use digital devices to support educational activities. CSBB-issued devices remain CSBB property and must be used, cared for and returned according to current asset management requirements.

Bring-your-own-device (BYOD) and other non-CSBB-owned devices remain the property and responsibility of the student, parent/carer, or device owner. CSBB is not responsible for the loss, theft, damage, repair, insurance, or replacement of non-CSBB-owned devices, except where required by law.

Responsible Use of Digital, Online and AI-Enabled Services

Students are expected to be responsible digital citizens.

Students are required to use approved services in accordance with this policy, school expectations and applicable laws by:

- accessing only approved services and resources
- accurately representing their identity when using digital and online services and maintaining the confidentiality of account credentials
- not entering, uploading or sharing personal, sensitive or confidential information about themselves or others, including students, staff, family members or members of the community, into AI-enabled services or other online platforms unless expressly authorised by the school for an approved educational purpose
- respecting privacy, consent, intellectual property and copyright requirements
- contributing positively to digital communities by treating others respectfully in all digital interactions and considering the impact of their digital actions on others
- thinking critically and demonstrating honesty and integrity in their learning by acknowledging sources and AI assistance as required
- seeking assistance or reporting concerns when unsure about online content or interactions.

Consequences of Non-Compliance

Access to CSBB-approved digital, online and AI systems and services may be limited, monitored, suspended or removed where there are concerns about safety, privacy, security, wellbeing or inappropriate use.

Disciplinary action may be undertaken against any student who is found to be inappropriately using provided digital, online or AI services or mobile devices. This includes excessive usage for personal reasons, knowingly accessing inappropriate or unsecure sites, creating and sharing inappropriate content, using services in a way that may create privacy or reputational risks and for legally prohibited and criminal activities.

Filtering

CSBB applies internet filtering, monitoring and security controls to support safe, appropriate educational use of digital and online services across schools. These controls are regularly reviewed and updated. Students must not attempt to bypass, disable or interfere with CSBB filtering, monitoring, firewall, security or access controls, including through personal hotspots, VPNs, proxy services, non-CSBB-owned devices or other methods.

Monitoring

Authorised personnel may monitor, review, log and analyse CSBB information and communication systems, networks, digital services, electronic communications and audit logs to maintain security, assess performance, investigate suspected policy breaches and meet compliance obligations. Monitoring is continuous and may be undertaken by CSBB or an authorised third party on behalf of the Director of Schools.

Use of AI-enabled systems, including prompts, outputs and associated analytics, may be monitored, logged and audited to support cybersecurity, privacy, safeguarding and policy compliance.

Students must promptly report inappropriate or unsafe content, or suspected cyber safety or security concerns, to a trusted adult or the school. Principals, or their authorised delegates, may review student online activity where there is a suspected policy breach, safeguarding concern or cyber security risk. Monitoring, investigation, parent/carer communication and resulting action will be undertaken with regard to the dignity, privacy, safety and wellbeing of all parties and in accordance with relevant CSBB policies and procedures.

Cyber Security

CSBB is committed to promoting safe participation in digital environments. Maintaining cyber security is a shared responsibility. Students must comply with current CSBB cyber security, authentication, identity management and access control requirements and must not bypass, disable, interfere with or circumvent any technical security controls implemented.

Students must keep their authentication credentials confidential and secure. Sharing, disclosing or using another person's account or credentials is prohibited. Staff must not create or allow practices that enable students or other users to access, guess or use another person's credentials.

Students must promptly report suspected cyber safety or security concerns to a trusted adult or the school.

Artificial Intelligence (AI) and Generative AI

CSBB recognises the educational opportunities presented by AI and Generative AI technologies and acknowledges associated risks. Students may use AI tools approved for use, aligned with Catholic values and human dignity, consistent with privacy obligations, and used in accordance with any AI guidance, standards or procedures. Staff may restrict or prohibit the use of AI tools in specific learning activities or assessment tasks.

Digital Communication

Digital communication should reflect the same standards of respect and conduct expected in face-to-face interactions.

Digital communications, records and content created, received, stored or transmitted using CSBB accounts, systems or networks, including AI-generated content, are the property of CSBB. Such information may be monitored, accessed, reviewed, retained or disclosed by authorised personnel in accordance with CSBB policies, governance requirements and applicable laws.

Student Acceptable Use Agreements

Schools may require students to acknowledge or sign local Student Acceptable Use Agreements. Such agreements will align with this policy, be developmentally appropriate, reflect local school contexts and operational requirements and be periodically reviewed.

Related Legislation

- Human Rights and Equal Opportunities Commission Act 1986 (Com.)
- Classification (Publication, Films and Computer Games) Act 1995(Com.)
- Copyright Act 1968 (Com.)
- Copyright Amendment [Digital Agenda] Act 2000 (Com.)
- Privacy Amendment (Private Sector) Act 2000 (Com.)
- Anti-Discrimination Act 1977 (NSW)
- Children and Young Persons (Care and Protection) Act 1998 (NSW)
- Crimes Act 1900 (NSW)
- Defamation Act 2005 (NSW)
- Workplace Surveillance Act 2005 (NSW)
- Privacy Act 1988 (Com.)
- Spam Act 2003 (Com.)
- NSW Ombudsman Act 1974
- Online Safety Act 2021

Review

The Policy and related Procedures/Processes will be reviewed by the relevant Workstream Lead and approved by the Director of Schools or, when required, the CSBB Board. The review will be undertaken every three (3) years unless there is a legislative or regulatory requirement to do so earlier.

Version

Version	Current Title	Approval Date	Commencement Date
3	Student Acceptable Use Policy: Digital, Online and Artificial Intelligence Services (new title for Student Acceptable Use Policy: Digital Devices, Network and Online Services)	October 2026	November 2026

Approved by: Danny Casey – Director of Schools

Date of next review: October 2029