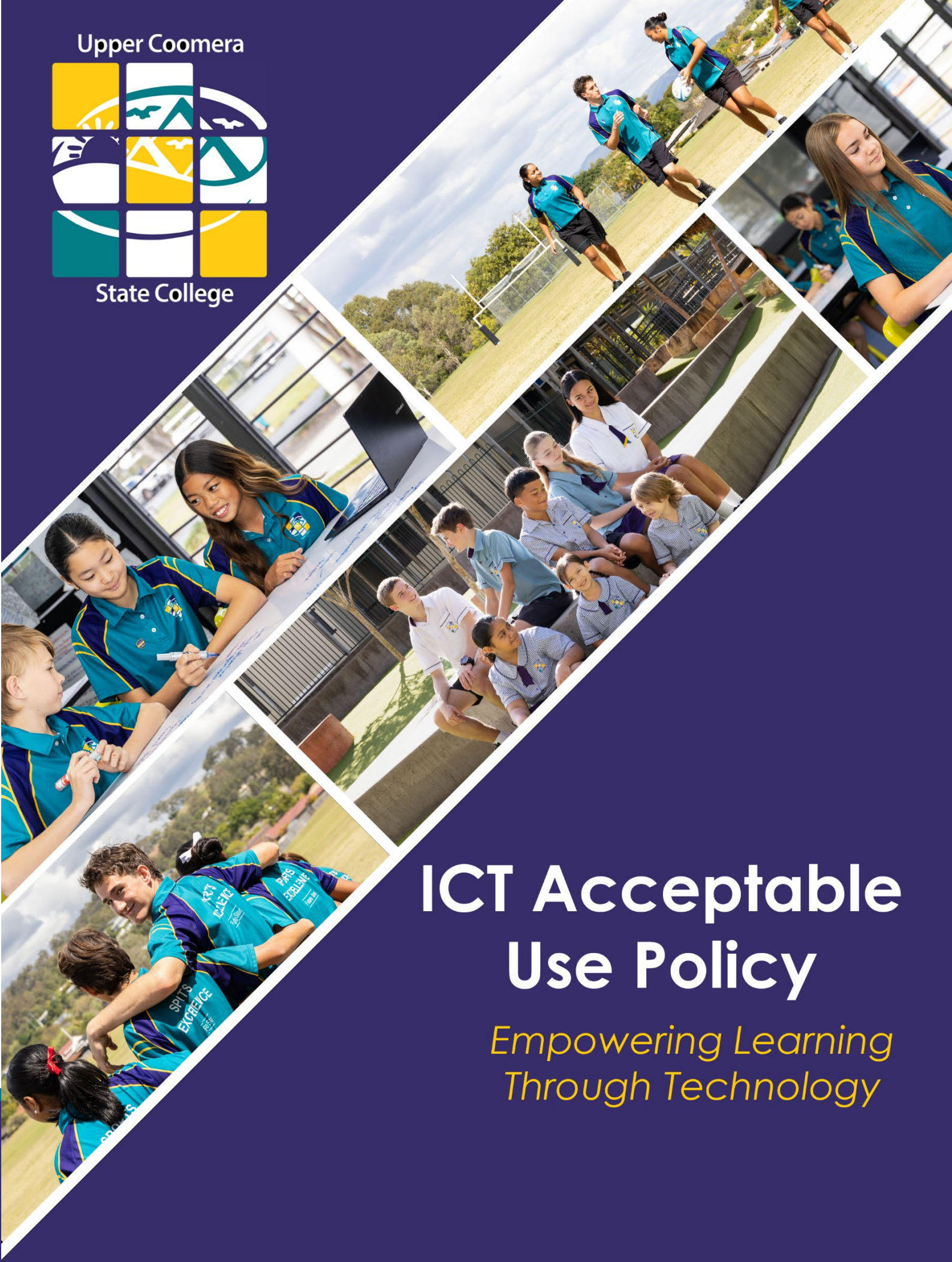
Upper Coomera State College



ICT Acceptable Use Policy

Empowering Learning Through Technology

Innovative • Committed • Inspired

Contents

Upper Coomera State College – ICT Acceptable Use Policy

Definition of "Device"

"Device" refers to any personally owned or school-provided technology used to access ICT services, including laptops, tablets, smartphones, and wearable technologies.

Acceptable Device Use

Students must follow school rules and the Responsible Behaviour Plan for Students when using their device:

- Be Responsible

- Be Respectful

- Be Safe

Students must comply with:

- The Department's Acceptable Use of ICT Network and Systems

- School's Code of Conduct

Examples of Acceptable Use:

- Participation in classwork and assignments set by teachers

- Developing 21st Century skills and digital literacy

- Creating text, artwork, audio, and video for educational purposes (as approved by staff)

- Researching school-related activities and projects

- Educational collaboration with peers, staff, parents, or experts

- Accessing online educational references and tools

- Engaging in the school's eLearning platforms

- Ensuring the device is fully charged each day for learning continuity

Students must be courteous and respectful when communicating or working online.

Unacceptable Device Use

Examples include:

- Engaging in illegal activities or accessing inappropriate material
- Downloading or distributing offensive or unauthorised content
- Using obscene, discriminatory, or inflammatory language
- Harassing, insulting, stalking or threatening others
- Damaging ICT equipment or wasting resources
- Plagiarism or copyright infringement
- Accessing private 3G/4G/5G or personal hotspots during school hours
- Using AI tools to complete work without approval
- Using the device's camera in inappropriate areas (e.g. toilets)
- Violating privacy by recording conversations or distributing personal content
- Sharing personal details online without valid educational purpose

School Responsibilities

Educate students on cyber safety, email etiquette, and safe device use

Monitor and filter internet content (Education Queensland's MIS)

Pre-assess and filter websites for learning tasks

Provide digital citizenship education

Enforce network and device use standards

Parent and Student Responsibilities

Understand behavioural and network access expectations

Report harmful content or misuse

Monitor out-of-school use of devices and cloud services

Recognise the value of ICT in education while understanding associated risks

Discuss and support safe digital behaviours and positive online reputation-building

Digital Citizenship

Students should:

- Be thoughtful content creators and respectful online participants
- Maintain a positive digital footprint
- Avoid posting harmful or offensive material
- Understand that online behaviour can form a permanent record

Parents are expected to reinforce these values at home.

Cybersafety

If a student encounters harmful or suspicious content:

- Notify a teacher or parent immediately

Students must NOT send, post, or forward:

- Confidential messages without permission
- Spam, hoaxes, or chain emails
- Inappropriate, threatening, or sexual content
- False, defamatory or misleading information

Web Filtering and Security

All school devices and network-connected personal devices are subject to Education Queensland's web filtering

Filtering protects against inappropriate sites, scams, malware, and identity theft

Students must report any inappropriate sites or suspected security breaches

Cloud Services and Emerging Technology

Only department-approved cloud services (e.g. OneDrive, Google Workspace) are to be used for school purposes

The use of unauthorised storage or communication apps (e.g., Discord, WhatsApp, TikTok) is not permitted during school hours

AI-generated content must only be used when approved and must comply with academic honesty standards

Privacy and Confidentiality

Students must not use another user's credentials

Accessing other students' files or personal drives is prohibited

Students must not disclose personal or staff information without consent

Intellectual Property and Copyright

All work must be original or properly attributed

Students must acknowledge all sources used in their work

Permission must be obtained before publishing another person's work

All publishing must be approved by the school principal or delegate

Monitoring and Consequences

Internet and device use may be audited at any time

Devices may be inspected following a security or misconduct report

Violations of this policy may lead to disciplinary action, including restricted access or loss of BYOD privileges

Resources for Parents and Students

- Department of Education Cybersafety Guidelines

- eSafety Commissioner