Rationale

To ensure our students are well equipped to function in, and contribute fully to our current and future society, Earnshaw State College provides opportunities for real world experiences to help students develop their skills in digital technology and the provision of learning opportunities for all students, to engage in science, technology, engineering and mathematics (STEM), including coding and robotics.

An essential tool for our college to provide these opportunities is the utilisation of intranet, Internet and network services. To ensure a safe and supportive learning environment, students need to accept the responsibility that comes with access to these resources, and students must understand that there will be consequences for inappropriate use.

Implementation - Conditions of Use:

Students must sign an agreement to use the Earnshaw State College ICT network, facilities and resources to:

- Complete assigned class work and assignments set by teachers
- Develop literacy, communication and information skills
- Author text, artwork, audio and visual material for publication on the Intranet or Internet, solely for educational purposes as supervised and approved by the college
- Conduct research for school activities and projects
- Communicate with other students, teachers, parents or experts in relation to school work
- Access online references such as dictionaries, encyclopaedias
- Collaborate, research and learn through Education Queensland's e-learning environment

In the agreement, students agree not to use the Earnshaw State College ICT network, facilities and resources to:

- Download, distribute or publish offensive messages or pictures
- Use obscene or abusive language to harass, insult or attack others
- Deliberately waste printing and Internet resources
- Damage computers, printers or the network equipment
- Violate copyright laws which includes plagiarism
- Use unsupervised internet chat
- Use online email services (e.g. hotmail), send chain letters or Spam e-mail (junk mail)
- Divulge their username and password to any other individual.
- Use another student or staff member's username or password to access the school's network, including trespassing in another person's files, home drive or e-mail.
- Divulge personal information (e.g. name, parent's name, address), via the internet or e-mail, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.
- Make deliberate attempts to access restricted files, disrupt the College network system, destroy data or gain unauthorised data.

In the agreement students agree that they will **NOT**:

- Use images of students in the College uniform, taken at College activities/lessons, or identifying the College without the written permission of the College Principal (eg. putting photos or video/s taken at school on Instagram, Snapchat, YouTube, Facebook or other social networking sites).
- Use USB or other memory storage devices to bring non-educational files onto the College network (eg games, music, images).
- Use College resources to play games, access or play unauthorised music, download applications or other forms of software, or to procure without the express permission of the College Principal.
- Use personal devices to create wireless hotspots to circumvent the secure College network.
- Use any electronic devices or the College network to bully or harass other students or staff.

In the agreement students agree that access to the Earnshaw State College network by student's wholly privately-owned ICT devices could compromise the integrity of the Education Queensland network, and is therefore not permitted.

Students need to be prepared for the possibility of unanticipated access to harmful information, materials or approaches from unknown persons via the internet (e.g. SPAM or viruses and Trojans with other files from the net). It is therefore a condition of use that students must report accidental access to offensive, illegal, harmful information and approaches from unknown persons via the Internet to the supervising teacher or school staff member.

Earnshaw State College reserves the right to restrict/remove student access to the intranet, extranet, Internet or network facilities if parents or students do not adhere to this network, facilities and equipment usage policy. This may also include other College behavioural consequences (e.g. Suspension) as outlined in our Student Code of Conduct and as seen as appropriate by the College Administration.

Definitions	
the network may be defined as:	• any location on the college domain, including all mapped network drives, college owned storage media devices, and government owned online data repositories (including virtual classrooms and blogs.)
unlicensed content may be defined as:	• a copy of digital media (sound, video etc.) where a student cannot prove original ownership.
inappropriate content may be defined as content that:	• advocates hate or violence • offers games or software whose content could be considered pornographic or offensive on the grounds of gender, ethnicity, religious or political beliefs • includes soft-core pornography • offensive, defamatory, discriminatory, malicious, pornographic or illegal
illegal content may be defined as content that:	• is illegal to access/be in possession of as per state or federal legislation.
authorised may be defined as:	• having direct permission by a teacher or adult supervisor, this may be in written or verbal form.
destruction may be defined as:	• an action that results in hardware/device requiring repair or replacement resulting in an expenditure of College resources (human/physical/financial) • malware and code infections
malicious may be defined as:	• intentional • premeditated
privately owned may be defined as:	• a laptop, tablet, smartphone or other device that has been purchased with non-departmental funds.
Inappropriate email use may be defined as:	• defaming, harassing, abusing or otherwise offending other internet and email users, individuals, government agencies or other organisations; • creating or distributing any form of malicious or deleterious material via the internet or email • attempting to obscure the origin of any message or downloading material under an assumed internet address or otherwise disguising a user's identity • forwarding unsolicited messages (spamming) or other junk email including chain email • inappropriate language used in emails