The Cathedral School of St Anne & St James TOWNSVILLE

Founded 1917

# Student ICT Acceptable Use

## School Governance

## 1. PURPOSE

The School provides network and internet access for use by students, allowing entry to a vast amount of information and resources. The network is provided and maintained for the benefit of all students. Students are responsible for good behaviour in relation to school–owned technology and bring your own devices while accessing the school network and when using the internet.

## 2. SCOPE

This procedure applies to all students and covers the use of school computers and other electronic devices, bring your own devices, internet access, email protocols, security of information and confidentiality requirements.

## 3. ROLES & RESPONSIBILITIES

| Position / Title | Area of Responsibility |
|---|---|
| Principal | • Ensuring the safe and effective use of ICTs within the school<br>• Ensure that any bullying, harassment, discrimination, harm, likely or suspected sexual abuse of students is to be investigated in accordance with the relevant School Policies.<br>• Apply disciplinary procedures in relation to inappropriate or misuse of ICT resources by students |
| ICT Manager/ICT staff | • Oversee the monitoring of ICT network and report inappropriate activity to the appropriate personnel. |
| Heads of Schools / Director of Boarding | • Apply disciplinary procedures in relation to inappropriate or misuse of ICT resources by students/boarders. |
| Teachers / All Staff | • Ensuring the safe and effective use of ICTs within the school<br>• Demonstrate safe, lawful and ethical behaviour when using the schools ICT network. |
| Students | • Demonstrate safe, lawful and ethical behaviour when using the schools ICT network<br>• Comply with this procedure and the Student ICT Acceptable Use Policy |
| Parent/guardians | • Are responsible for ensuring students understand the school's ICT access and usage requirements, including the acceptable and unacceptable behaviour requirements. |

## 4. PROCEDURE

The Cathedral School provides students with computer/electronic facilities for educational use. Students may use these facilities for educational and research purposes, including for class work, assignments and for the development in skills using a computer. Students are also provided with email facilities to be used for school related business.

Student access is a privilege, not a right and inappropriate use will result in the privilege being withdrawn or other consequences. The school's computer system records all email and internet usage and should an issue arise in relation to email and internet usage, the relevant records will be accessed.

Students must know, understand and respect the laws relating to privacy, intellectual property, copyright and ownership of data, system security and defamation rights. The school may take legal action against those who breach these laws or against those who bring the school into disrepute at any time, whether during school or outside of school.

### 4.1 Student responsibilities for using the school's ICT facilities

- Only software purchased or approved by the school, and installed by the school, can be used on school equipment. It is illegal to copy copyrighted software contrary to the Licence Agreement. No software on the school computer system may be copied.
- Students must not abuse or deliberately misuse ICT equipment.
- The use of material that is illegal or which would be regarded by reasonable persons as offensive is not permitted.
- Students should be aware that all internet accesses are logged.
- Use of the School's social media channels must be in accordance with the *'Social Media Terms of Use Procedure'*.
- If students are found misusing their access to the internet, intranet or electronic communication tools by, for example, sending chain letters or abusive letters or accessing offensive material, they will be referred for disciplinary action.
- The school's email or social media systems is not to be used for bullying or harassing another person. Students found using the school's system or any non-school electronic device, including mobile phones, for cyber bullying should expect disciplinary action.
- Usernames and passwords are to be kept private by the student and not divulged to any other individual (e.g. a student should not share their username and password with fellow students).
- Students cannot use another student or staff member's username or password to access the school's network, including not trespassing in another person's files, home drive or e-mail.
- Students are to employ caution with the use of mobile devices e.g. USBs, particularly as these devices can store significant numbers and sizes of files some of which may be unacceptable at school and contain viruses.
- Students must not use any application or network protocol to bypass, damage or harm the school's ICT Network filtering policies.

- Students are not to access, modify or destroy data, files, and programs belonging to other users.
- Students are not to use electronic devices with a camera in any place where a camera would normally be considered inappropriate. This includes in change rooms and toilets or any situation which may cause embarrassment or discomfort to others.

### 4.2 Students responsibilities when using the internet (whether at school or beyond school)

It is against School policy and the legal rights of others, to disclose or discuss any personal information without the knowledge and consent of that person, or to bully or misuse technology whether using technology provided by the school or through the use of personal technology.

- No student is to identify or share the personal information of teachers and other staff including names, addresses and telephone numbers of staff etc.
- No student is to publish any identifying or defamatory opinions/photos they may have about staff, fellow students or the school.
- No student should post photos or recording or themselves or others without their knowledge and consent.
- Students should not divulge their own personal information (e.g. name, parent's name, address, phone numbers), via the internet or through electronic communications, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.
- Students are expected to respect the privacy and ownership of others' work at all times. This includes not plagiarising information they find on the Internet and presenting it as their own work, or copying work of other students, with or without permission.
- Students must maintain privacy and confidentiality and respect the personal rights of others. Only post data that is suitable for everyone to see (parents, teachers and friends).

Student disciplinary action will be carried out in accordance with relevant behaviour management procedures for breaches which took place at school. The school cannot enforce the legal rights of other people (including students) when and if they are breached beyond school time. This is a matter for parents.

The school may take legal action against those who breach the school's legal rights (privacy, intellection property, copyright and defamation rights) and the legal rights of staff whether the incident occurs during or beyond school.

It is acceptable for students to use school computers and network infrastructure for:

- Assigned class work and assignments set by teachers
- Developing appropriate literacy, communication and information skills
- Authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes
- Conducting general research for school activities and projects

- Communicating or collaborating with other students, teachers, parents or experts in relation to school work
- Accessing online references such as dictionaries, encyclopaedias, etc.
- Researching and learning through the schools e-learning environment.

Students are to report any violent, dangerous, racist or inappropriate content received or viewed to their Teacher.

### 4.3 General ICT Requirements

#### 4.3.1 Copyright

Only software purchased or approved by the school, and installed by the school, can be used on school equipment. It is illegal to copy copyrighted software contrary to the Licence Agreement. Software copying must be in accordance with legal requirements, and 'pirate' software is not permitted on any school owned computer.

#### 4.3.2 School liability

The school owns all messages and transmissions conducted through its system and therefore are legally responsible for all communications. Students should be aware that the school's computer system records all email and internet usage and should an issue arise in relation to email and internet usage, the relevant records would be accessed.

#### 4.3.3 Technology Harassment

Students should be aware that email harassment and/or technology harassment can occur on any of the grounds of discrimination. The school will not tolerate email and/or internet harassment. Any issue involving harassment or discrimination could result in disciplinary action.

#### 4.3.4 Access

Computer systems at the school are protected by password access as well as physical barriers where possible. At no time should third parties be given unsupervised access to school records.

#### 4.3.5 Viruses

The school attempts to prevent and/or detect viruses by ensuring suitable virus detection software is maintained on computer networks. Please contact the IT Team if you detect a virus on school equipment.

#### 4.3.6 Security

Students should report any security breach, including suspected security weaknesses and software malfunctions, to their Teacher immediately. Students should be aware that student involvement in a security breach is considered serious and may result in disciplinary action.

Students are required to keep logon details confidential. The owner of the school account is responsible for all activity on that account.

### 4.3.7 Emails

Students are expected to use their school email account while communicating on school business. Students are to use language that is appropriate for school when communicating via email.

### 4.3.8 Acceptable Internet Use

The school uses internet filtering software which restricts the inappropriate access to websites for students. Student's access to internet sites is cached so that inappropriate use can be identified. Internet access can be monitored "real-time" during school hours, or by a report generated after the event.

## 4.4 Monitoring of network use including internet, intranet and emails

The school monitors access to and usage of the ICT network. For example, e-mail monitoring will occur to identify inappropriate use, protect system security, maintain system performance, and determine compliance with school procedures and legislation.

The school reserves the right to restrict student access to network services if access and usage requirements are not met or are breached. However restricted access is not to disrupt the provision of the educational program within the school. For example, a student with restricted school network access may be allocated a stand-alone workstation to continue educational program activities.

The School may deny access to the internet without warning for any device which breaches the schools' ICT network filtering policies. The user will need to contact ICT staff to determine the cause and remediation.

ICT monitoring, recording and audits are conducted to:

- Ensure that the systems and networks are functioning properly
- Ensure compliance with school policies/procedures
- Protect the confidentiality and integrity of information held by the systems and networks
- Protect against unauthorised access or use.
- Investigate conduct that may be illegal or adversely affect the school or its employees/students

The school uses an internet filter which logs inappropriate use of internet resources and inappropriate language used in electronic communications.

## 4.5 Student Misuse of ICT Networks

- Student offensive language identified by the school's monitoring program or misuse is to be reported to the relevant Head of School or Director of Boarding.
- The identification of any bullying, harassment, discrimination, harm, likely or suspected sexual abuse of students is to be reported to the Head of School's and investigated in accordance with the relevant *Student Protection Manual.*

- Inappropriate use of social media channels will result in disciplinary actions taken by the school, this includes any use which can cause significant business or reputation damage to the school.

### 4.6 Private Device Access

Students connecting private devices to the school network are required to:

- Follow ICT Procedures.
- Have secure passwords and the required security applications and virus software installed
- Ensure the device is used in a lawful, responsible and ethical manner
- Ensure all software and other material complies with Copyright and Intellectual Property requirements
- Understand that the school may restrict or deny access to the network by any private device if there is any suspicion that the integrity of the network might be at risk
- Understand that the school may conduct security audits and scans of any private device connected or proposing to connect to the network if at any time the security of the network is at risk.

## 5. DEFINITIONS

- ICT – Information Communication Technology
- Electronic Communications – includes any form of electronic communication (emailing, texting, social networking)

## 6. REFERENCED & ASSOCIATED DOCUMENTATION

**Legislative**

- Copyright Act 1968 (Commonwealth)
- Privacy Act 1988 (Commonwealth
- Child Protection Act 1999

**Procedures & Forms**

- Behaviour Management Policy - Junior School
- Behaviour Management Policy - Middle and Senior School
- Student Protection Manual
- Privacy Policy
- Social Media Terms of Use Procedure