CATHOLIC EDUCATION
Archdiocese of Canberra & Goulburn

STUDENT ACCEPTABLE USE OF ICT POLICY

Title	Student Acceptable Use of ICT Policy
Description of policy	This policy sets out expectations and obligations for using Information and Communications Technologies (ICT) to support students' education in a secure, safe and supportive environment, while decreasing the risk of network vulnerability, or student exposure to inappropriate and offensive material or behaviours.
Required because	CECG Networks and online teaching and communications carry risks for schools to manage, from network security to privacy and child protection. This policy provides a clear framework for schools and agreements for students and parents to abide by.
Description of changes	Minor changes to reduce title length and clarify Acceptable Use Agreement and Personal Digital Device Agreement. Personal Digital Device Agreement reformatted so schools do not need to enter any information. Acceptable Use Agreements are signed by students each year. Schools may provide families with Personal Device Agreements as required or as part of standard beginning of year paperwork.
Applies to	☐ Organisation-wide ☒ Specific: Schools
	☐ Staff only ☒ Students only ☐ Staff and students
Status	☐ New ☐ Major revision of existing document ☒ Minor revision of existing document

Publication location	Intranet and Public Website
Related documents	Student Acceptable Use Agreement Personal Digital Device Use Agreement Personal Digital Device Agreement
Intranet category	Child Protection and Student Welfare Information and Communications Technology
Review date	June 2025
Trim reference number	R591209

Approval authority for this version: **Approval date:**	School and Family Services Area Leader 01/06/2023
Accountable authority	School and Family Services Area Leader
Responsible officer	Child Protection Manager

1. Summary

1.1 This policy sets out expectations and obligations for using Information and Communications Technologies (ICT) to support students' education in a secure, safe and respectful environment. It highlights obligations for staff, students and parents in Catholic Education Archdiocese of Canberra Goulburn (CECG) schools.

1.2 The policy applies to all digital devices, applications and networks used by students in CECG schools, or outside school premises for education purposes.

2. Student Acceptable Use of ICT Policy

2.1 Students must use school Information and Communications Technology (ICT) for acceptable use only.

- Acceptable use includes work related to the student's curriculum and educational needs, and incidental personal use (e.g. internet searching) that does not interfere with the learning environment or school operations and network security.

2.2 Parents and students (if age appropriate) must read and sign the Student Acceptable Use Agreement.

- Generally, students from Pre-Kindergarten through Year 2 will be considered too young to sign the Acceptable Use Agreement. A parent/guardian will sign for these students ensure they have explained the agreement to their child.

2.3 Students who wish to use personal devices at school, and their parents/carers, must sign a Personal Digital Device Use Agreement. It outlines expectations and responsibilities to use personal devices in a way that does not interfere with the learning environment or create risks for network security and student information.

2.4 Student access to CECG ICT is a privilege and access may be revoked for not following acceptable use standards. Other consequences may also apply depending on the severity of the breach (e.g. cyberbullying, which is against the CECG Bullying and Harassment Policy).

2.5 Information created, communicated, stored or accessed using CECG digital devices, applications, and networks may be monitored by the school or Catholic Education Office.

2.6 All students remain bound by Territory, State or Commonwealth laws, including anti-bullying laws, laws about pornography including child pornography, anti-discrimination laws, privacy laws, and laws concerning criminal use of technology.

3. Catholic Education Office Responsibilities

3.1 The Catholic Education Office (CEO) will:

- Review the use of ICT from time to time to ensure it is acceptable
- Take lawful action to protect the security of its assets, facilities and networks
- Take lawful action to fulfil its duty of care to students including blocking Internet sites, restricting a user's access, and confiscation of devices.

4. School Principal Responsibilities:

4.1 School principals will:

- Ensure that a Student Acceptable Use Agreement and (if relevant) a Personal Digital Device Use Agreement is signed annually by parents/guardians and students (Year 3 and above) before a student is allowed to access school ICT.
- Ensure students receive appropriate instruction so they can understand and comply with the Acceptable Use Agreement and this policy.
- Ensure students receive appropriate instructions regarding network security when using digital devices, applications and networks.
- Seek informed parent consent before allowing access to digital applications that share student data.
- Provide education for students that focus on safe and respectful behaviours on the internet protective behaviours when accessing online environments, and possible dangers of communicating personal information.
- Endeavour to monitor student compliance with the Acceptable Use Agreement, to investigate alleged breaches of the Acceptable Use Agreement by students, and to implement appropriate consequences; and
- Work with the CEO to monitor use of digital devices, applications and networks, and inform students that monitoring may occur.

5. Student Responsibilities

5.1 Students will abide by the responsibilities set out in the Student Acceptable Use Agreement and Personal Digital Device Use Agreement.

6. Parent responsibilities

6.1 Parents must read and sign the Student Acceptable Use Agreement and the Personal Digital Device Use Agreement (if applicable) before their child is allowed to use school ICT.

6.2 Parents are responsible for supervising student use of digital devices and applications, and internet use while the student is at home.

6.3 Parents must not

- Use their child's CECG provisioned username or protected password to access the CECG network, digital devices or applications. These are for student use only.
- Photograph, record or post images, sound or information about teachers or students at CECG schools without the permission of a teacher and the permission of each person being photographed or recorded.
    - CECG schools may have students whose identity is protected and endangered by sharing their image or location.
- post or forward information, images or videos that:
    - Claim to represent the school without permission
    - Might bring people or the school into disrepute
    - Contain inappropriate or hurtful material about members of the school community.

7. Personal Digital Devices

7.1 Each school will determine whether personal digital devices will be allowed at school and, if so, which devices are allowed. All personal digital devices brought to the School will be

governed by this Policy. CECG and its schools consider that personal devices allowed at school should be used for educational purposes rather than personal use.

7.2 Parents/Guardians of students wishing to authenticate a personal device on the school's network must sign a Personal Digital Device Use Agreement.

7.3 Schools are not responsible for maintaining or charging personal digital devices.

7.4 The school will not be liable for loss or damage to personal digital devices. Students are NOT to lend their personal digital devices to others while at school. Arrangements must be made to store devices when those devices are not in use. Schools will develop their own storage approach.

7.5 Schools are not responsible for personal digital device use outside school hours. However, unacceptable use outside school hours may connect with school and interfere with the learning environment, such as cyberbullying of other students. In this case, schools need to respond in line with the Bullying and Harassment Policy or Behavioural Support, Suspension, and Expulsion Policy.

8. Monitoring

8.1 The content and usage of student email and other electronic communications may be examined from time to time by the school Principal, the Catholic Education Office, or a third party on the CEO's behalf.

8.2 All student messages and files on the CECG network will be treated as education related and may be monitored. Students should not expect that any message or file transmitted or stored on CECG digital devices, applications, or network will be private.

8.3 Students should be aware that CECG is able to monitor their use of the Internet when accessed through their school network. This includes the Internet sites and content accessed and the length of time spent using the Internet.

9. Social Media

9.1 While at school or using the CECG network on school or personal devices, students must only access or contribute to social media sites if:

- Those sites the content is solely related to an educational context
- If permission is given by a teacher to access those sites
- If parents have provided informed consent to access the digital application.

9.2 Students must only communicate with their teachers through formal school communication channels and learning platforms, use of school social media accounts or groups for communication is not permitted, and students should not invite teachers to join their personal networks.

10. Definitions

10.1 **Acceptable use:** includes all uses related CECG business that comply with relevant laws and CECG policy, and incidental personal use (e.g. internet searching and personal administration) that complies with CECG policy and does not interfere with work, system operations or security.

10.2 **Networks:** includes local area networks, connections to external electronic networks and subscriptions to external network services.

10.3 **Digital Devices:** include desktop computers, laptops, tablets, mp3 players, iPods, USB storage devices and mobile phones, regardless of who they belong to, that are brought onto the CEO or school property or to school activities, or that are connected to the CECG network or facilities.

10.4 **Applications:** refers to any application software that can be used by a computer, mobile device, or tablet, which may be cloud or client based

10.5 **Inappropriate material:** means material which is inappropriate or harmful for children and includes:

- Child abuse images: depictions of children being sexually abused or posing inappropriately.
- Pornography: depictions of adults engaged in sexual activity.
- Nudity: depictions of detailed nudity.
- Violence: depictions of violence that is particularly strong in impact.
- Illegal activity: content which promotes or instructs in criminal activity.
- Terrorist related material: content that advocates terrorist activities.
- Other material that may require an adult perspective.

10.6 **Incidental personal use:** is defined as use by an individual student for occasional personal communications provided that such use is lawful and complies with this Policy.

10.7 **Information and Communication Technology (ICT):** means all computer hardware, software and applications, systems and network infrastructure.

10.8 **Internet:** refers to the global network of multi-platform smaller computer networks which allow users to access information, communicate and collaborate electronically.

10.9 **Personal device:** means a piece of electronic equipment, such as a laptop computer or a mobile phone, that is small and easy to carry and that belongs to an individual rather than being CEO or school property.

10.10 **Social media:** are any form of online publication or presence that allows interactive communication. Social media sites include but are not limited to:

- Micro-blogging sites, e.g. Twitter
- Social networking sites, e.g. Facebook
- Video and photo sharing sites, e.g. YouTube, Instagram, Tik Tok
- Weblogs, including corporate or personal blogs
- Forums and discussion boards, e.g. Reddit
- Wikis, e.g. Wikipedia
- Multiplayer gaming sites
- Virtual world sites

11. Related Documents and Legislation

11.1 Related CECG Documents:

- Student Acceptable Use Agreement
- Personal Digital Device Use Agreement
- Personal Digital Device Agreement

11.2 Online resources for Esafety

- Australian Privacy Principles
- CyberSmart Challenge for Primary Students
- Bullying No Way: Online Safety and Online Bullying guidance
- Esafety Commissioner

12. Contact

12.1 For support or further questions relating to this policy, contact the CECG School and Family Services team.