CATHOLIC EDUCATION
Archdiocese of Canberra & Goulburn

STUDENT ACCEPTABLE USE OF DIGITAL DEVICES, APPLICATIONS AND NETWORKS POLICY

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 Digital Devices, Applications and Networks

2.1 Students must use digital devices, applications and networks for acceptable use only. Acceptable use includes all legal uses related to the student's curriculum and educational needs. It also includes incidental personal use (e.g. internet searching) that complies with this policy and does not interfere with school, or system operations and security.

2.2 Student access to CECG digital devices, applications and networks 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).

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

2.4 Personal devices using CECG networks may be searched and/or confiscated if the principal believes, on reasonable grounds, there is a threat to a person or system security, or the device has been used for unlawful conduct or a serious breach of CECG or school policy or codes of conduct. In certain circumstances, information may be used in legal proceedings.

2.5 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.

2.6 Students must read and sign (if age appropriate) Student Acceptable Use Agreement, which must be co-signed by a parent/guardian. 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 and document that they have read and explained the agreement to their child.

3. Catholic Education Office Responsibilities

3.1 The Catholic Education Office (CEO) will:

- review the use of digital devices, applications and networks from time to time to ensure it is acceptable.
- take lawful action to protect the security of its assets, facilities and networks; and

- 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 Principals Responsibilities:

4.1 School principals will:

- Ensure that an Acceptable Use Agreement is signed annually by parents/guardians and students (Year 3 and above) and placed on record in the school before a student is allowed to access digital devices, applications and networks at school.
- 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.

6. Parent Responsibilities

6.1 Parents must read and sign the Acceptable Use Agreement and the Use of Personal Devices Agreement (if applicable) before their child is allowed to use CECG digital devices, applications, or networks.

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;
- use their personal devices to photograph or record video or sound of teachers or students at CECG schools without the permission of a teacher and the permission of each person being photographed or recorded;

- post or forward information about or images or videos of teachers, or students (other than their own) without the permission of all the people the information is about, or who are pictured in the images or video;
- post any images of students in uniform or otherwise identified with the school unless written permission has been received from the principal;
- 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
  - could be used to identify members of the school community (such as passwords, phone numbers and addresses) without their permission and without carefully considering the possible unwanted consequences.

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 personally owned computer or other approved device to the school's network must sign a Personal Digital Device Use Agreement. It outlines expectations and the end user's responsibility in managing the device. Students in Years 3 or above should also read and sign this agreement.

7.3 Devices owned by students may be searched and/or confiscated if the principal believes, on reasonable grounds, that there is a threat to a person or system security or the device has been used or involved with unlawful conduct or a serious breach of the Acceptable Use Agreement. This may occur whether the device was provided by the school, purchased by parents as part of a school initiative, or is individually owned.

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

7.5 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.

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:

9.2 those sites the content is solely related to an educational context, if permission is given by a teacher to access those sites, and if parents have provided informed consent to access the digital application.

9.3 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, 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 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 Information, Communications and Technology Service Area.