Title	Staff Acceptable ICT Use Policy
Description of policy	This policy sets out the expectations and obligations for staff using Catholic Education Archdiocese of Canberra and Goulburn digital devices, applications and networks. It applies to all CECG workers, in all CECG workplaces and work-related activities.
Required because	CECG networks and digital devices and applications carry risks to manage, from network security to workplace misconduct, privacy and child protection. This policy provides a clear framework for staff and obligations for staff to abide by.
Description of changes	Removed the requirement for schools to manage and archive signing of the Staff Acceptable Use Agreement. All staff acknowledge and accept this policy upon commencement in a process managed centrally by the People and Culture team. Schools should still remind staff of acceptable ICT use, this policy and its requirements.
Applies to	☒ Organisation-wide ☐ Specific (location, schools/ELCs&SACs, Service Area)
	☒ Staff only ☐ Students only ☐ Staff and students
Status	☐ New ☐ Major revision of existing document ☒ Minor revision of existing document

Publication location	Intranet
Related documents	Social Media Policy Student Acceptable Use of ICT Policy Cyber Security Policy
Intranet category	Information, Communications, and Technology
Review date	01/01/2027
Trim reference number	R592004

Approval authority for this version:	People and Culture Area Leader
Approval date:	30/01/2025
Accountable authority	People and Culture Area Leader
Responsible officer	People and Culture Officer

1. Summary

1.1   This policy sets out the expectations and obligations for workers using Catholic Education Archdiocese of Canberra and Goulburn (CECG) digital devices, applications and networks. It applies to all CECG workers, in all CECG workplaces and all work-related activities. It also applies to the use of personal digital devices on CECG networks.

2. Staff Acceptable Use of ICT Policy

2.1   Workers must use all work-related ICT resources for acceptable use only. This includes all CECG digital devices, applications and networks and personal devices that access CECG networks or applications.

2.2   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.

2.3   All workers must comply with all relevant Territory, State or Commonwealth laws and CECG policies. This includes anti-bullying legislation, laws regarding the possession or transmission of pornography including child pornography, harassment, anti-discrimination legislation, privacy laws, and laws concerning the improper use of technology with criminal intent.

2.4   Staff must read and accept this policy upon commencement. The recruitment team in the Catholic Education Office (CEO) is responsible for ensuring all staff accept this policy and storing records of staff acceptance.

2.5   Information created, communicated, stored or accessed using CECG digital devices, applications or networks is subject to monitoring by CECG.

2.6   Personal devices using CECG networks may be searched and/or confiscated if the Service Area Leader or Principal believes, on reasonable grounds, that 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 policy or codes of conduct. In certain circumstances, information may be used in legal proceedings.

2.7   CECG is not responsible for the physical security, maintenance or repair of a personal devices that are used in the workplace.

3. Specific Staff Obligations

3.1   When using CECG digital devices, applications and networks, workers must:

- seek advice from the ICT Service Area before obtaining any software, applications or digital devices for use in their school or Service Area
- seek informed consent from parents before introducing students to new digital applications that share student data
- exercise good judgment, particularly in relation to cyber security
- use appropriate language and images
- communicate with students in a manner consistent with their role and responsibilities and in relation to educational/school matters

- not access, upload, download, send, circulate, display or respond to any of the following materials:
  - sexually related or pornographic messages or material including that which contains thoughts and feelings with overly familiar or sexual connotations
  - violent or hate-related messages or material
  - threatening, defamatory, obscene or harassing messages or material
  - racist, gender biased or other offensive messages or material
  - subversive or other messages or material related to inappropriate or illegal activities
- report in a timely manner any inappropriate use of digital devices, applications or networks by another worker.

4. Student and Parent Communications and Messaging

4.1 Work-related communication with students and parents should be through formal work channels, for example through work email addresses or Compass.

4.2 If there are reasons for workers to communicate with students or their families using digital devices, applications or networks for reasons other than educational/school purposes, workers must discuss this with their principal or manager beforehand.

4.3 Digital learning applications (e.g. Seesaw, Google Classroom, and Microsoft Teams) that allow communication with parents must only be used to communicate about student learning. Where possible, messaging features for parents should be disabled.

4.4 Schools may develop additional communication procedures or practices to guide parent and teacher communication.

5. Appropriate Use of Social Media

5.1 Whenever using social media, staff must comply with the CECG Social Media Policy.

6. Definitions

6.1 **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.

6.2 **Digital Devices:** includes 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.

6.3 **Applications:** refers to any application software that can be used by a computer, mobile device, or tablet, whether cloud- or client-based.

6.4 **Incidental personal use:** is use by an individual staff member for occasional personal communications provided that such use is lawful and complies with this Policy.

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

6.6 **Personal electronic device:** means a piece of electronic equipment, such as a laptop computer or a mobile phone that belongs to an individual rather than being CEO property.

6.7 **Social media:** are any form of online publication or presence that allows interactive communication. Social media sites include:

- micro-blogging sites, eg Twitter
- social networking sites, eg Facebook
- video and photo sharing sites, eg YouTube, Instagram, Tik Tok
- weblogs, including corporate or personal blogs
- forums and discussion boards, eg Reddit
- wikis, eg Wikipedia
- multiplayer gaming sites
- virtual world sites
- dating sites or applications.

6.8 **Workers:** all people carrying out work for CECG including employees (permanent, casual, and temporary), contractors and sub-contractors, volunteers, apprentices, work experience students, or a minister, priest, or other religious leader or member of a religious organisation.

7. Related Documents and Legislation

7.1 Related CECG Documents:

- Student Acceptable Use of ICT Policy
- Social Media Policy
- Cyber Security Policy

8. Contact

8.1 For support or further questions relating to this policy, contact People and Culture.