catholic education south australia

SOUTH AUSTRALIAN COMMISSION FOR CATHOLIC SCHOOLS

ST THOMAS MORE SCHOOL ELIZABETH PARK

ICT Acceptable Use

Policy

Version 1.2

Contents

SOUTH AUSTRALIAN COMMISSION FOR CATHOLIC SCHOOLS
PO BOX 179 TORRENSVILLE PLAZA SOUTH AUSTRALIA 5031
TELEPHONE: (08) 8301 6600 FACSIMILE: (08) 8301 6611

www.cesa.catholic.edu.au February 2022

1 Purpose

This policy establishes best practice for the use of Information and Communication Technology (ICT) within Catholic Education South Australia (CESA).

2 Scope of Policy

This policy applies across the Catholic Education Offices, Catholic schools and Centres in South Australia and includes:

- All information processed, stored, and transiting ICT facilities.
- All ICT equipment, hardware and software used in the conduct of the ICT function within CESA.

This policy applies to the following:

- All Catholic schools, the Catholic Education Offices and Centres in South Australia.
- All staff and students within all Catholic schools and Catholic Education Offices in South Australia; and
- All parents, volunteers and others who may have cause to utilise ICT facilities provided by CESA.

3 Policy

Acceptable Use

All individuals who access, use or otherwise engage CESA ICT resources are required to:

a) Respect the rights of all individuals, including other users.

b) Only use or modify CESA ICT resources for authorised purposes and not in breach of relevant laws, regulations and/or professional contractual obligations.

c) Not use CESA computer or network equipment for non-commercial personal purposes beyond a reasonable amount or to the detriment of CESA or its values.

d) Not access, distribute, store or display illegal, pirated or offensive material.

e) Not use CESA computer or network equipment for unauthorised personal financial or commercial gain.

f) Not misrepresent the views of CESA via use of CESA ICT resources.

g) Not conduct activities that consume excessive network bandwidth.

h) Report suspect or actual security breaches to CEO ICT in a timely manner.

i) Maintain the security and confidentiality of information gathered or collected by CESA in accordance with the Information Classification Policy and Guideline.

j) Adhere to all policies, procedures and guidelines as published and updated periodically.

Secure System Access and Use

To protect access to CESA ICT resources, individuals are required to:

a) Select long and strong passwords that adhere to parameters as defined in the Access Management Policy.

b) Not share CESA-provided or self-selected passwords with other individuals.

c) Keep personal and CESA-provided systems, used to access CESA information, free from known vulnerabilities by keeping up-to-date with vendor provided security updates.

d) Maintain operational and up-to-date antivirus on personal and CESA-provided systems used to access CESA systems or information.

e) Securely store passwords that provide access to CESA systems or information.

f) Only use the accounts provided by CESA for their own individual use.

g) Only use the accounts provided by CESA for CESA related purposes.

h) Not bypass or attempt to circumnavigate CESA's security controls or protection mechanisms.

i) Not introduce malicious software such as viruses, worms, ransomware or trojans into the CESA environment.

j) Not use hacking tools (including sniffing, scanning, password guessing or exploitation) when accessing, using or otherwise engaging with CESA ICT resources.

k) Do not reuse CESA passwords for private use applications.

Monitoring and Compliance

a) CESA will monitor its ICT resources for compliance with this policy and breaches of this policy constitute misuse of CESA information and information systems.

b) The **ICT Acceptable Use Policy – Misuse Schedule** provides some examples of activities that constitute misuse of ICT resources. If misuse of ICT resources is detected or suspected, relevant disciplinary provisions including the revocation of system privileges, disciplinary action up to and including dismissal may be invoked.

c) CESA may refer serious matters or repeated breaches to the Director ICT, Human Resources, head of relevant business division or the appropriate external authorities which may result in disciplinary and/or civil and/or criminal proceedings.

d) CESA has a statutory obligation to report illegal activities or corrupt conduct to appropriate authorities and will cooperate fully with the relevant authorities.

e) To the extent allowed by law, CESA is not liable for loss, damage or consequential loss or damage arising directly or indirectly from the use or misuse of any ICT resources.

4 Definitions

CEO - means either or both of the Adelaide and Port Pirie Catholic Education Offices, as the context permits.

CESA - means Catholic Education South Australia, including any School, Centre or the CEOs, as the context may permit.

ICT - Information and Communications Technology is a term that includes any facilities used to compute, communicate and to store information electronically. This may include and is not limited to desktop, laptop, and tablet computers, computer servers, electronic storage devices, network and telecommunications equipment and associated software.

SACCS - South Australian Commission for Catholic Schools (SACCS)

School - means any South Australian Catholic school.

Staff - means any employee of CESA, including contractors, casual staff and outsource provided staff with contact with CESA provided ICT facilities.

5 Related documents/links

The following documents are to be read in conjunction with this policy.

- SACCS Cyber Security Policy
- SACCS Cyber Security Framework
- SACCS Acceptable Use Guideline
- SACCS Privacy Policy
- Associated School or CEO policies and procedures

6 Responsibility for implementation, monitoring, and continual improvement

Responsibility for the implementation, monitoring and review of this policy is vested at the level appropriate to the following roles:

Responsibility for	Diocesan schools	CEO	Separately Governed schools[1] for consideration
Approval	SACCS	SACCS	Board or equivalent
Monitoring	School Performance Leader / Director ICT	Director ICT	Board or equivalent / per delegations
Reviewing	Director ICT	Director ICT	In accordance with governing framework
Implementing	Principal	Director ICT	Principal

1: For separately governed schools, this responsibility matrix is for guidance. It is the expectations of SACCS that equivalent controls exist within the schools' governance framework.

This policy must be reviewed at least every three years from the date of approval, or when a major change that has the potential to change risk exposure.

The review must evaluate the policy for suitability, effectiveness, relevance and alignment with SACCS business goals.

7 Revision Record

Document Title	SACCS ICT Acceptable Use Policy
Document Type	Policy
Document Date	November 2023
Revision Number	V1.3
Policy Owner	Director, Information Communications and Technology
Contact	phil.proctor@cesa.catholic.edu.au (08) 8301 6600
Approval Authority	SACCS
Review Date	November 2026
Revision History	November 2023: Reviewed to align with Information Stewardship initiative. February 2022: Policy review June 2020: Version number updated to 1.01 September 2018: Document inception