catholic
education
south australia

SOUTH AUSTRALIAN COMMISSION
FOR CATHOLIC SCHOOLS

ICT Acceptable Use

Guideline

Version 1.10

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 November 2023

1 Purpose

This document provides a set of guiding statements to establish acceptable use practices that apply to the provision and utilisation of ICT facilities within Catholic schools, Centres and the Catholic Education Office (CESA).

2 Scope

The scope of this guideline applies across CESA for any person accessing or using ICT facilities provided by CESA.

This guideline supports the SACCS ICT Acceptable Use Policy.

3 Standards and Appropriate Use Guidelines

3.1 Acceptable Use of ICT Facilities

The use of, or access to, ICT facilities incorporates an expectation of responsible behaviour, acting ethically and responsibly in all dealings with others.

3.1.1 Incidental Personal Use

Incidental personal use is permitted if the use:

- Conforms to SACCS, school and CEO policies and standards.
- Does not hinder the staff member's productivity and in the case of student does not interfere with student learning.
- Is approved by an appropriate authority as the case may apply.
- Is legal and complies with CESA regulatory and contractual requirements.

3.1.2 Appropriate Use

Use of ICT facilities requires that persons:

- Access only the information necessary in the execution of their duties. Any access rights not required are to be reported through management to the relevant ICT support resource as soon as practical.
    - Staff should be aware that access to information not required to perform their work poses a personal risk and added responsibility for that information.
- Recognise obligations implied and explicit regarding the maintenance of confidentiality, security, integrity and privacy of information for which they either have access to or has responsibility for.
- Comply with all legal and regulatory obligations as applies at the time. Specifically in relation to privacy, copyright and software licensing obligations.

- Maintain secure password practice:
  - Maintain a secure password known only to themselves i.e. no password sharing.
  - Maintain discrete passwords for individual systems, using a password management system as necessary and as recommended or endorsed by an appropriate ICT authority.
  - Use passwords that comply with the SACCS Access Management procedure.
  - Notify the appropriate ICT authority immediately if suspicious activity regarding access or passwords is suspected.
- Use multifactor authentication as implemented and in accordance with SACCS access management (password and passphrase) requirements.
- Only access information required for the execution of your role within CESA. Report excess access not required for your role, or that of your subordinates to ICT in the approved manner.
- Use only the email account allocated to yourself. Use of another's email account is not permitted and may result in disciplinary action.
- Maintain awareness of privacy and legal obligations in relation to still and video photography. No images are to be taken without the express consent of the individuals concerned.
- Maintain awareness of the SACCS cyber security policy, procedures and expectations to maintain high standards of security.
- Report evidence of, or suspicion of unauthorised access, use and other suspicious activity in the use of ICT assets and information assets to the school and CEO authorities.
- Report access to inappropriate material, accidental or otherwise.
- Ensure the safe keeping of all equipment and the data stored within the ICT provided in the course of your work.
  - Staff are required to report any loss of equipment as soon as practical.
  - Equipment to be safely transported, not left unattended and not visible during transit. For example, store equipment in car boot, not on a seat or car floor.
- Users of CESA ICT facilities are not permitted to download or install software unless it has been approved by an appropriate ICT authority and declared safe and licenced for use within CESA.

3.1.3 Unacceptable Use of ICT Facilities

Inappropriate activity includes that which:

- Is illegal or contrary to regulatory obligations.
- Seeks to gain unauthorised access to any resource or entity, including another's email account and/or system resources.
- Without authorisation destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of computer-based information and/or information resources.
- Transmits or causes to be transmitted, communication that is offensive or threatening, constitutes harassment, discrimination, vilification, defamation or bullying.
- Deliberately access, view, download, forward any offensive information or material that is illegal, abusive, of a sexist, racist, or offensive nature including extremist, intolerant, pornographic, profane or contrary to the generally accepted standards for the use of ICT facilities.
- Transmit or facilitate the transmission of unsolicited email, otherwise known as spam.
- Contravenes SACCS, school or CEO licence obligations and agreements.
- Transmits sensitive, private or confidential information to external entities unless that information is encrypted or otherwise protected by technique approved by a recognised CESA ICT authority in information security.

4 Monitoring and Compliance

To ensure compliance:

- CESA entities will implement an acceptable use agreement as a condition of granting access to ICT facilities. A checklist and templates for such agreements are included as Appendices.
- All users of CESA provided ICT facilities will by implication, accept that authorised ICT staff will monitor activity by automated and manual means to ensure compliance and the highest levels of security are maintained.
- CESA will provide ICT staff tools to the proactively protect ICT facilities. Protections will include but not limited to the provision of system wide threat protection solutions, alerting and monitoring.

  Nonetheless the technical protections, adherence to the principles outlined in this guideline will enhance the overall protection required and expected.

5 Definitions

CEO - means either of the Adelaide and Port Pirie Catholic Education Offices.

CESA - means Catholic Education South Australia, including any Catholic school, Centre or the CEO.

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, tablet computers, computer servers, electronic storage devices, network and telecommunications equipment and all associated software and all supporting peripheral devices.

SACCS - South Australian Commission for Catholic Schools.

School - means any South Australian Catholic school.

Staff - means any employee of CESA, including casual employees and contractors.

6 Related documents/links

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

- SACCS Cyber Security Policy
- SACCS Cyber Security Framework
- ICT Acceptable Use Policy
- SACCS Privacy Policy

7 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:

	Diocesan Schools	**CEO**	**Separately Governed Schools for consideration**
Approve	SACCS	SACCS	Board or equivalent
Monitor	School Performance Leader / Director ICT	Director ICT	Board or equivalent / per delegations
Review	Director ICT	Director ICT	In accordance with governing framework
Implement	Principal	Director ICT	Principal

NOTE: 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 CESA goes through a major change that has the potential to change risk exposure.

8 Revision Record

Document Title	ICT Acceptable Use Guideline
Document Type	Guideline
Document Date	January 2024
Revision Number	V1.10
Owner	Director Information and Communications Technology
Contact	Director Information and Communications Technology phil.proctor@cesa.catholic.edu.au (08) 8301 6600
Approval Authority	SACCS
Review Date	January 2027
Revision History	January 2024: reviewed in line with the Information Stewardship initiative. April 2020, review, update to version 1.01 September 2018, document inception, version 1.0

Appendix A. Checklist of items to be covered in Acceptable Use Agreements.

CHECKLIST OF MATTERS TO BE COVERED IN SCHOOLS' ACCEPTABLE USE AGREEMENTS Exact wording and concepts to be adapted to suit the age and development of the relevant students in each School context.		
1.	**Scope of Agreement** with particular emphasis on use of personal devices at school, and out of hours conduct. This Agreement covers: ▪ all users of ICT within the school ▪ all use of school ICT facilities ▪ all use of personal ICT devices to access the school network or facilities. ▪ conduct both during and outside of school hours.	□
2.	Acceptable Conduct: ▪ conduct consistent with the Catholic ethos. ▪ behave ethically and responsibly in all dealings with others. ▪ observe obligations regarding confidentiality and privacy. ▪ select and maintain a secure password and ensure you do not provide the password to anyone else. ▪ Do not attempt to gain unauthorised access to anyone else's account or user information, or otherwise attempt to defeat any security controls. ▪ restricted use of devices that record others or take photos. ▪ report any suspicions of unauthorised or inappropriate access to the school and the CEO. ▪ treat equipment with care. ▪ physical control and safe keeping of devices supplied to them by the school.	□

3.	Unacceptable Conduct ▪ send or publish any statement, image or other material that is offensive or threatening, or could constitute harassment, discrimination, vilification, defamation or bullying. ▪ knowingly access, download, store, send or publish any material that is pornographic. ▪ do anything that you know, or reasonably suspect could contravene the law, including without limitation downloading material in breach of copyright. ▪ send or help to send unsolicited bulk email (spam). ▪ open or download any attachment, or access any link, that you reasonably suspect may contain a virus, malware or other computer contaminant. ▪ install unlicensed or non-approved software onto any supplied computers or communication devices. ▪ use ICT Facilities to cheat or plagiarise. ▪ use ICT Facilities to store or download files for personal use.	□
4.	Staying Safe Online Reporting to an adult if a student accesses a website or sees something online that makes them feel uncomfortable	□
5.	Specifics of what to do in the event of cyberbullying (victims and bystanders)	□
6.	Personal Devices Personal ICT devices that access material on the school network and services: ▪ must be protected with a secure password. ▪ may be monitored by school and/or CEO personnel. ▪ must be provided to the School/CEO authorities for the purposes of assisting the authorities to determine whether inappropriate conduct has occurred. ▪ usage of personal devices must comply with guideline statements as if the equipment was supplied by the school. ▪ Must permit the school/CEO to manage access to CESA information.	□

7.	Students may use ICT facilities for incidental personal use, provided such use is minimal and does not interfere with the performance of their learning.	□
8.	Students are encouraged to collaborate within the system; however, this should be done in a safe manner. Students should obtain a teacher's permission prior to establishing contact with participants not associated with their school. Teachers should record any approvals granted for external collaboration.	□
9.	When posting material in social media forum students should be reminded that such activity may be considered public, not private.	□
10.	Consequences of breach of this agreement may result in loss of privileges including loss of access to ICT facilities or further disciplinary procedures as appropriate.	□

Appendix B. Sample Student Acceptable Use Agreement.

STUDENT USER AGREEMENT

Insert College Logo

[School Name]

This User Agreement sets out the terms on which you may access information and communication (ICT) facilities provided by the school.

By signing this Acceptable Use Agreement, you (including parents/guardians in the case of students under 18 years) are agreeing to the terms set out in this Acceptable Use Agreement, including the consequences of any breach of the terms.

1. Privacy Consent

Information that you transfer or store using the school's computing services may have implications for Privacy and you are reminded to read and understand the school's Privacy policy.

2. Acceptable Use

You agree that you will comply with all requirements as set out in this Agreement, and any acceptable use documentation that may be provided to you by your school.

3. Monitoring

You agree that authorised school staff and authorised Catholic Education Office staff can and will monitor your use of ICT facilities to ensure compliance with acceptable use guidelines and practices as defined and communicated to you.

4. Suspension or termination of use and other consequences

Inappropriate use of ICT services and facilities may result in the termination of access.

Disciplinary consequences may also apply.

5. Agreement and Consent

I, the student named below, hereby agree to comply with all requirements as set out in this Agreement and in the Acceptable Use Standard and all other relevant laws and restrictions in my access to the various ICT resources through the school and Catholic Education SA network.

NAME: ___________________________ CLASS: _____________

SIGNATURE: ______________________ DATE: _________________

Parent/Guardian Consent (for students under 18 years of age)

As the parent or legal guardian of the student named above, I consent to the student accessing the various information and communication technology resources through the school and) on the terms set out in this Agreement and related documentation provided.

NAME: ____ DATE: _________________

SIGNATURE: ____