

Cloud Computing Policy

Version 1.03



Contents

Contents	2
1 Purpose	3
2 Scope of Policy	3
3 Policy	3
4 Definitions	5
5 Responsibility for implementation, monitoring, and continual improvement	6
6 Revision Record	6
7 Related documents/links	7

1 Purpose

This policy enables a standardised approach to the adoption and use of cloud-based services (Cloud) for the provision of storage, compute and software application facilities.

The policy establishes an expectation that Cloud services may be considered as an option when sourcing Information and Communication Technology (ICT). In considering Cloud services, appropriate attention must be paid to the security and privacy implications of the information collected and stored by the service.

This policy outlines requirements and minimum standards to be applied when sourcing ICT services delivered from a Cloud service provider.

2 Scope of Policy

This policy applies to the CEO, Catholic Schools and Centres in South Australia (CESA). This includes all variations of Cloud services whether they are short term required for single purpose engagement or on a subscription basis, and up to and including long term contractual arrangements.

3 Policy

It is the policy of SACCS that:

1. Sourcing options for the provision of ICT services may include Cloud service providers.
2. Prior to procurement, an evaluation must be conducted and needs to consider the following:
 - a. Non-disclosure agreements
 - b. Data ownership throughout the agreement
 - c. Data storage location
 - d. Legal prevalence
 - e. Data breach notification
 - f. Data breach penalty
 - g. Data breach management
 - h. Data retention, deletion & destruction
 - i. System and Information Security

Additional consideration to factors such as, but not limited to true cost, functionality, risk, efficiency are to be included in evaluation prior to procurement.

3. Information that will be processed, stored or transiting Cloud services will be classified in accordance with approved standards and guidelines.

The resultant Information Classification documentation is to be preserved for future reference and the classification reviewed on a regular timetable.

4. A Privacy Impact Assessment is conducted in all instances.
The “Privacy Impact Assessment” template is available for use.
5. A risk assessment is completed prior to acquisition of all ICT systems, with additional rigour to be applied to Cloud services.
6. Roles for managing cloud vendor relationships and service delivery must be clearly defined and communicated. Moving data assets into the cloud may require business support realignment with roles and responsibilities shifting from adoption of Cloud services.
7. Cloud sourcing options must consider the following criteria:
 - The value and sensitivity of the information to be stored and processed in the cloud, as defined by the Australian Privacy Act.
 - Security and protection of data in transit and at rest. Including:
 - Security and Privacy obligations required by law.
 - Security obligations required by SACCS.
 - Security provided by the application itself.
 - Security provided by the Cloud provider’s infrastructure.
 - Identify and log management (including access to logs).
 - SACCS entities must be permitted to conduct security assessments on Cloud services, or review reputable third-party security audit reports, on a regular schedule, at least annually.
 - System availability times meet business requirements.
 - System resilience and recovery times meet business requirements.
 - Backup options meet business requirements.
 - Data retrieval fees are known in advance and accepted.
 - Cloud agreement entry and exit costs are known and accepted in advance.
 - Data destruction on agreement exit is guaranteed.
 - Data management once the Cloud service is no longer required.
8. Hosting location. A strong preference is to be given to solutions hosted within Australia.
 - Information rated as “High” in terms of confidentiality are not permitted to be stored in offshore locations.
 - Information rated “Medium” in terms of confidentiality may be stored in an offshore location subject to full risk evaluation and written justification of the decision to use such a facility.
 - Information rated “Low” in terms of confidentiality must have appropriate protections applied in accordance with SACCS risk tolerances and policies.
 - Guidance on how to classify information is available in the reference document “Information Security Classification Guideline”.
9. For the use of Cloud storage services:

- Use of free, personal and/or unmanaged cloud storage facilities are prohibited for the use where CESA information is involved. For example, but not limited to Dropbox, Google Drive, Apple iCloud, Box, others.

For clarity, if John Citizen has both a personal OneDrive and school OneDrive, the use of the personal OneDrive to store CESA information is not permitted.

New Cloud services require evaluation and approval prior to use.

4 Definitions

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

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

Cloud Services or Cloud Computing (Cloud) - refers to a computer service that is accessed through a network without the need to acquire, own, and operate dedicated infrastructure, software and facilities.

There are typically three cloud service models:

Infrastructure as a Service (IaaS) where a vendor provides the computer hardware, processing power, memory, data storage and network connectivity.

IaaS physical hardware may be shared with multiple customers, with each customer being virtually separated using software.

IaaS helps a customer to build and manage data requirements as it grows, without having to own and manage servers.

Platform as a Service (PaaS) builds on IaaS by also managing operating systems and services on behalf of the customer.

PaaS enables the development of custom-built applications online without having to be concerned with the infrastructure.

Software as a Service (SaaS) builds on PaaS where the vendor also provides the software applications.

In this example the customer subscribes to the application. For example, Office 365, Civica.

Cloud Right - refers to an approach where preference is given to Cloud services; however due consideration is given to the entire business case need including information protection.

ICT - Information and Communications Technology and includes computing facilities, communication devices and software applications.

SACCS - South Australian Commission for Catholic Schools (SACCS)

School - means any South Australian Catholic school.

Staff - means any employee of CESA.

5 Responsibility for implementation, monitoring, and continual improvement

Responsibility for implementation, monitoring and review of the 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 expectation 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.

6 Revision Record

Document Title	Cloud Computing
Document Type	Policy
Document Date	January 2024
Revision Number	V1.03
Policy Owner	Director, Information and Communications Technology
Contact	phil.proctor@cesa.catholic.edu.au (08) 8301 6600
Approval Authority	SA Commission for Catholic Schools
Review Date	January 2027
Revision History	January 2024: Reviewed in line with Information Stewardship initiative. February 2022: Review and update to version 1.02 June 2020: Review and update to version number 1.01 December 2018: Document inception, version 1.0

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 2024

7 Related documents/links

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

- SACCS Cyber Security Policy
- SACCS Cyber Security Framework
- SACCS Privacy Policy
- SACCS Information Security Classification Guideline
- The (US) National Institute of Standards and Technology (NIST), Definition of Cloud Computing
- Risk management standard AS/NZS ISO 31000.
- Privacy Impact Assessment template