Adelaide Central School of Art

Cyber Security Policy

Policy Id	A010
Original Version	July 2025
Current version	Approved by the Board of Governors, 28 July 2025
Scheduled review date	July 2028
Threshold Standard	6.2
Responsible person/s	Operations Manager and Chief Executive Officer

1. Introduction

Adelaide Central School of Art (**ACSA**) acquires, develops and maintains computing networks, infrastructure and applications. These resources are intended to service the ACSA community, including direct and indirect support of teaching and learning, research, administrative, student and campus life, security and other general needs including the free exchange of ideas.

Cyber security enables confidentiality, integrity and availability of information by providing protection against malicious and accidental threats. Cyber security threats take advantage of weaknesses in technology, people and processes to harm information.

ACSA's approach to cyber security is informed by the South Australian Cyber Security Framework (SACSF).

1. Purpose

The purpose of this Cyber Security Policy is to protect the confidentiality, integrity, and availability of Adelaide Central School of Art's (ACSA) information systems and data. It establishes the framework for managing and mitigating cyber security risks, safeguarding student and staff data, and ensuring compliance with applicable Australian laws and standards.

2. Scope

This policy applies to:

All staff (permanent, casual, visiting),

Students,

Contractors,

Volunteers,

Third-party service providers,

Any individual who accesses the school's IT resources.

3. Objectives

Prevent unauthorised access to ACSA's digital infrastructure and data.

Ensure appropriate use of IT resources.

Support compliance with the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs).

Align with the Australian Cyber Security Centre's (ACSC) Essential Eight strategies.

Respond effectively to cyber incidents.

4. Responsibilities

4.1 Consumers and Students

- Consumers and Students are responsible for reporting potential cyber security incidents to the Operations Manager.
- Use IT systems responsibly.
- Complete mandatory cyber security training.

4.2 ACSA staff and contractors

- Complying with procedures in place to protect information assets.
- Reporting risks to Operations Manager and CEO.
- Reporting potential cyber security incidents to Operations Manager and CEO.
- Complete mandatory cyber security training.

4.3 Management

- Management manages relevant cyber security risks and are accountable for compliance with relevant cyber security standards.
- Implement technical and procedural controls.
- Monitor threats and manage incidents.
- Conduct regular vulnerability assessments and risk audits.
- Provide cyber security training and awareness.

4.4 IT staff and contractors

- Complying with relevant IT and cyber security standards and local operating procedures.
- Assist to identify and develop suitable cyber security frameworks, standards and local operating procedures.
- Monitor IT systems and services for potential cyber security risks and threats.

5. Policy Statements

5.1 Access Control

- All users must authenticate using unique credentials.
- Privileged access (e.g., admin rights) must be tightly controlled.
- Multi-factor authentication (MFA) must be used for all remote access and sensitive systems.

5.2 Data Protection

- Personal and sensitive data must be stored securely and encrypted where appropriate.
- Data must be backed up regularly and tested.
- Only authorised individuals may access student or staff data.

5.3 Device Security

- All devices connecting to the ACSA network must have up-to-date antivirus software and operating system patches.

Operating systems and software must have ongoing support by Microsoft or Apple (ensures to latest security features and updates). Microsoft is ending support for Windows 10 in October 2025

- BYOD (Bring Your Own Device) is permitted only under defined security conditions.

Access for BYOD is primarily through the Wi-Fi through the portal, not direct access to the network. In cases such as staff BYOD, access is to the curriculum server, which does not include access to any company or sensitive information.

5.4 Acceptable Use

- IT systems must only be used for lawful and school-related purposes.

- Prohibited activities include:

  Downloading pirated material,

  Circumventing security controls,

  Using the network to harass, defame, or harm others.

5.5 Incident Management

- All cyber security incidents must be reported immediately to the Operations Manager and CEO.
- All cyber security incidents will be reported to the Board of Governors.
- A formal Incident Response Plan will be followed, including notification to the Office of the Australian Information Commissioner (OAIC) if a notifiable data breach occurs.

5.6 Third-Party Access

- Third parties (e.g. cloud vendors, contractors) must comply with ACSA's cyber security and privacy requirements.
- Data sharing agreements must be in place.

5.7 Training & Awareness

- Cyber security awareness training must be conducted annually for all staff and students.
- Additional training will be provided in response to new threats or technologies.

6. Compliance

Failure to comply with this policy may result in disciplinary action, including access restrictions, dismissal, or referral to law enforcement.

7. Review

This policy will be reviewed annually or following a major security incident, legislative change, or technology shift.

9 Related Documents

ACSA Privacy Policy and Procedures
ACSA Privacy Statement
ACSA Records Management Policy and Procedure
ACSA Misconduct Policy
Australian Privacy Principles

Australian Privacy Principles Guidelines
Privacy Act 1988 (Cth)

10 Review

This policy will be reviewed at least once in every 3 year period commencing on the date of approval of this policy.

11. Contact

For any questions or to report an incident, contact:

Operations Manager / Cyber Security Officer

Email: facilities@acsa.sa.edu.au

Phone: 8299 7300