Cyber and Information Security Policy

Code and Version Control:	ID150 Version 2.0
Policy Owner:	Chief Executive Officer
Date Approved by Board of Directors:	2 November 2026
Scheduled Review Date:	November 2029
Related Policies and Documents:	• Business Continuity Policy and Procedure • Critical Incident Management Policy and Procedure • Privacy Policy and Procedure • Student and Staff Usage of Internet and Email Policy and Procedure • Business Continuity Plan • Information and Technology Resources and Recovery Plan

Legislative and Regulatory Compliance

APAC's Cyber/Information Security Policy is designed to support compliance with applicable Australian legal and regulatory obligations, including the Higher Education Standards Framework (Threshold Standards) 2021, the Tertiary Education Quality and Standards Agency Act 2011, the Education Services for Overseas Students Act 2000 (ESOS Act), the National Code of Practice for Providers of Education and Training to Overseas Students 2018, the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and the Notifiable Data Breaches scheme under the Privacy Act.

Purpose

The purpose of this Policy is to set out the information security policies that apply to the Australian Performing Arts Conservatory (APAC) to protect the confidentiality, integrity, and availability of data.

This Policy establishes APAC's cyber security risk management and responsibilities, it applies to APAC and all authorised users of APAC information, systems and digital services, including staff, students, contractors, consultants, temporary workers, education agents, service providers, visitors, and any third parties granted authorised access.

This Policy aims to protect APAC's information from unauthorised access, loss, or damage, intentional or otherwise while ensuring seamless access to academic resources by students.

APAC adopts a risk-based approach to cyber and information security governance. Cyber security risk is treated as an enterprise risk and integrated into APAC's governance, risk management and compliance processes. Responsibility for oversight rests with the Board of Directors and the Finance, Audit and Risk Management (FARM) Committee, while APAC Management, GEDU Group IT, staff, contractors and third-party providers are accountable for implementing, maintaining and complying with information security controls appropriate to their roles and responsibilities.

Australian Performing Arts Conservatory ABN 11 009 772 481
Registered as an Australian Institution of Higher Education PRV14046 CRICOS Provider Number 03897G

Scope

This Policy is broad and applies to all stakeholders at APAC that hold or process APAC information, including:

- Current, prospective and former students;
- Staff;
- Third parties (e.g., consultants, contractors, education agents, partners and suppliers);
- Visitors.

This Policy applies to all APAC information assets in any form, including paper records, electronic records, cloud-hosted information, systems, endpoints, removable media, backups, credentials, logs, and third-party managed platforms.

Principles

Policy Statement

- APAC recognises the importance of cybersecurity. It is committed to ensuring all Institute activities involving Information Technology are appropriately defended against cybersecurity threats.
- APAC is committed to the appropriate use of Information Technology and Services to support its learning, teaching, research, administrative, and service functions.
- Management of cyber security risk requires a concerted effort across all APAC and APAC recognises that successful implementation of cybersecurity relies on having a well-informed user community combined with effective management procedures.
- This overarching policy is supported by this recognition, and it provides principles for APAC's continuous enhancement in terms of operational practice, action plans, technology controls and education programs around the concern of cybersecurity.
- APAC's approach to information security is informed by the Australian Cyber Security Centre (ACSC) Essential Eight, the ACSC Information Security Manual (ISM), applicable TEQSA / ESOS obligations, and risk management best practices.

Information Security Objectives

- To ensure the confidentiality, integrity, and availability of APAC information including personal information and sensitive information handled by APAC, in accordance with applicable Australian privacy laws and business, legal, regulatory and contractual obligations
- To provide the resources required to develop, implement, and continually improve the information security management system.
- To manage third-party suppliers who process, store, or transmit information to reduce and manage information security risks.
- To implement a culture of information security and data protection through effective training and

Australian Performing Arts Conservatory ABN 11 009 772 481
Registered as an Australian Institution of Higher Education PRV14046 CRICOS Provider Number 03897G

awareness.

- To ensure timely identification, reporting, investigation, response, recovery and lessons learned for cyber incidents and privacy breaches, including escalation to GEDU Group (parent organisation) support functions where applicable

Information Security Policy Framework

- The key pillars of APAC's information security framework are cyber security risk management, incident and breach management, governance and assurance; information and records management; access and identity management; third-party security management; business continuity and disaster recovery; awareness and training; and continual improvement.
- The specification of cyber security controls is incorporated into relevant IT standards or as separate cyber security standards.
- APAC will have sufficient IT and cyber security standards to facilitate the effective implementation of cyber security controls across all IT infrastructure, systems, and applications.
- Standards will be developed in consultation with key stakeholders to support business requirements, provide adequate cyber security risk mitigation, and align with the cyber security strategy.
- Standards will be updated as required to reflect changes in security controls.

Cyber Security Risk Management

- Cyber security controls seek to reduce cyber security risk by either reducing the likelihood or impact of an incident or both.
- APAC will continue to identify and treat cyber security risks by implementing and following preventive measures:
    - Internet, website, and email filtering;
    - Enterprise Endpoint Detection and Response;
    - Change request control and ITIL framework;
    - Minimum password length of **12 characters** and Multi Factor Authentication (MFA) mandate for all privileged access, remote access, and cloud services
    - Endpoint and system management and monitoring;
    - Security controls in application and patch management;
    - Restricted administrative privilege;
    - Regular backups;
    - Maintaining a register of key information assets;
    - Establishing a framework for performing cyber security risk assessments aligned with APAC's Enterprise Risk Management Framework;
    - Incorporating cyber security risk identification and assessment into processes impacting

the use and processing of APAC information;

- Maintaining a register of cyber security risks with related controls;
- Review information security and cyber security risks at planned intervals and following significant incidents, material system changes, onboarding of new suppliers, regulatory changes, or major business process changes
- Implementing and strengthening controls to reduce risk;
- Evaluating the effectiveness of controls;
- Make staff and contractors aware of the security requirements of APAC IT resources and services and take precautions to safeguard their access to systems against any unauthorised use.
- Information classification and handling controls;
- Centralised logging, monitoring and alerting appropriate to service criticality;
- Vulnerability assessment and patch governance;
- Periodic access reviews and controls over privileged access;
- Third-party due diligence and contractual security controls;
- Backup protection, including restore testing;
- Joiners, movers and leavers access lifecycle controls;
- Secure software development and change management controls;
- Data retention, secure disposal, and records management controls.
- Application of Encryption controls - Encryption of data at rest for confidential and restricted information (e.g., AES-256 or equivalent). Use of TLS 1.2 or higher for all data in transit. Encryption of portable media and endpoint devices such as laptops.

Identity and User Access Management

APAC will maintain formal identity and access management processes to ensure access to information and systems is authorised, monitored, reviewed and removed in a controlled and auditable manner.

User access controls will include:

- Formal approval processes for granting, modifying, reviewing and removing access.
- Access granted only where a valid business, academic or operational requirement exists.
- Unique user accounts for all authorised users.
- Prohibition of shared accounts except where technically required, formally approved and appropriately monitored.
- Service accounts must have an identified owner, documented purpose, minimum necessary privileges and appropriately protected credentials, and must be periodically reviewed.

- Multi-factor authentication (MFA) for privileged, remote and cloud-based access.
- Support for modern authentication mechanisms, including passkeys, passwordless authentication technologies and phishing-resistant authentication methods, where technically feasible and supported by the underlying platform.
- Authentication controls will be periodically reviewed to ensure alignment with industry best practices and organisational risk requirements.
- Privileged access rights must only be assigned where necessary for authorised duties and restricted to the minimum level required.
- Privileged and administrative accounts must be separately managed, monitored and periodically reviewed.
- User access rights must be reviewed following role changes, transfers, termination or extended absence.
- General user access permissions must be reviewed and formally certified by the relevant Asset or Service Owner at least every six months.
- Immediate removal or suspension of access following termination, withdrawal of authorised access or identification of inappropriate or excessive access.
- Timely modification of access following changes in employment status, responsibilities or operational requirements.
- Monitoring, logging and review of privileged account activities.
- Dormant, inactive or generic accounts must be periodically reviewed and disabled or removed where no longer required.
- User access review outcomes and remediation activities must be documented and retained.
- Segregation of duties must be implemented wherever practical to reduce the risk of fraud, error, unauthorised activity or misuse of information.
- Access to confidential, restricted, personal, student, staff, financial or sensitive information must be restricted to authorised personnel with a legitimate business requirement.
- Temporary, contractor and third-party access must have a defined expiry date, be periodically reviewed and be removed immediately when the approved requirement or engagement ends.
- Where feasible, access management processes should be automated to improve consistency, accuracy and auditability.

Asset and Service Owners are responsible for approving access to systems under their control, participating in periodic access reviews and ensuring that access remains appropriate to the user's role and responsibilities. Failure to comply with access management requirements may result in restriction or removal of access privileges and may be managed in accordance with applicable APAC policies, procedures and disciplinary processes.

Australian Performing Arts Conservatory ABN 11 009 772 481
Registered as an Australian Institution of Higher Education PRV14046 CRICOS Provider Number 03897G

External Storage Devices, Removable Media and Data Transfer Controls

The use of removable media and external storage devices presents an increased risk to APAC information and must be appropriately controlled.

APAC will minimise the use of removable media wherever approved secure cloud, collaboration or network storage services are available.

USB storage device access will be blocked by default on APAC-managed systems. Access may be granted only in exceptional circumstances where a documented business or academic requirement exists and approval has been provided by the relevant manager or Information Owner and GEDU Group IT or its delegated authority. Approved access must be time-bound and periodically reviewed, and temporary access must be used wherever technically feasible.

Approved USB access must be removed promptly when the authorised requirement ends, the approval expires or the associated risk is no longer acceptable.

Users:

- Must not connect unauthorised USB devices, external hard drives or storage media to APAC systems.
- Must not store confidential, restricted, personal, student, staff, financial or sensitive information on removable media unless formally approved.
- Must use GEDU Group IT-approved encryption on removable media containing Confidential, Restricted, personal or sensitive APAC information.
- Must ensure approved removable media is physically protected from loss, theft and unauthorised access.
- Must scan removable media for malicious software before use where technically feasible.
- Must securely delete or destroy information stored on removable media when no longer required.
- Must immediately report any loss, theft or suspected compromise of removable media.
- Must comply with secure disposal requirements.
- Must not use personally owned removable storage devices to store or transfer APAC information. Any exceptional use must be formally risk-assessed and approved by the relevant Information Owner and GEDU Group IT or delegated authority.

APAC reserves the right to restrict, block, monitor or disable removable media functionality on corporate systems where appropriate.

Artificial Intelligence (AI) Platform Governance and Oversight

APAC recognises Artificial Intelligence (AI) as an emerging technology that can provide educational, administrative and operational benefits, while also introducing information security, privacy, legal, regulatory, intellectual property, academic integrity and reputational risks.

APAC will manage the use of AI technologies through a risk-based governance approach designed to

ensure AI is implemented and used securely, ethically, lawfully and transparently.

Users must:

- Use only APAC-approved or GEDU-approved enterprise Artificial Intelligence (AI) platforms and services for business, operational or academic purposes.
- Not access, use or process APAC information through unauthorised AI applications, browser extensions, websites, mobile applications, plug-ins or consumer AI services.
- Not upload, input, disclose or process Confidential, Restricted, personal, student, employee, safeguarding, health, financial, commercially sensitive or regulated information through public, consumer or unauthorised AI services. Processing such information through an approved enterprise AI platform requires an approved use case and appropriate contractual, privacy, access-control and security safeguards.
- Verify the accuracy, appropriateness and relevance of AI-generated outputs before use.
- Ensure AI-generated outputs do not replace appropriate professional judgement, decision-making, approval processes, academic assessment, compliance review or management oversight.
- Ensure significant decisions supported by AI remain subject to appropriate human review and approval.
- Remain accountable for all decisions, actions, communications and outputs generated with the assistance of AI technologies.
- Comply with all applicable privacy, copyright, intellectual property, contractual, regulatory, academic integrity and information security obligations when using AI tools.

APAC will:

- Permit only approved enterprise AI platforms for processing APAC information.
- Require documented Information Security, Privacy, Compliance and Legal assessments, proportionate to risk, before implementing a new AI-enabled service or enabling significant AI functionality.
- Assess AI vendors through the applicable Information Security, Compliance team and business-owner review processes before approval
- Periodically review approved AI platforms to ensure continued compliance with privacy, security, legal and operational requirements.
- Monitor emerging AI-related risks, legal requirements, threat intelligence and good-practice guidance relevant to the use of AI technologies.
- Require contractual controls prohibiting APAC information, prompts, uploaded files, outputs and metadata from being used for external model training, unrelated analytics, service improvement or third-party purposes without APAC's explicit prior written approval. Any inability to obtain these protections must be documented and risk-assessed before approval.
- Unauthorised AI tools, websites, applications, browser extensions and services will be blocked

by default on APAC-managed systems where technically feasible. Any exception must be documented, risk-assessed, approved and time-bound.

Human Oversight and Accountability

Artificial Intelligence is intended to support, and not replace, human decision-making.

Proportionate and meaningful human review is required before materially relying on AI-generated outputs, particularly where they are used in:

- Academic activities and student-related decisions.
- Financial activities or financial reporting.
- Regulatory, compliance or legal activities.
- Information security activities.
- Policy development and governance decisions.
- Any decision that may significantly impact students, staff, partners or APAC operations.

Users remain fully accountable for all actions, decisions and outcomes produced with the assistance of AI technologies.

Incident Reporting

Any unauthorised use of AI platforms, suspected information leakage, privacy breach, exposure of sensitive information, AI-generated misinformation, security weakness or other AI-related incident must be reported immediately through APAC's Information Security Incident Management process.

Failure to comply with this section may result in restriction of access to AI services, disciplinary action and other actions considered appropriate by APAC.

Incident and Privacy Breach Management

- An incident or breach is any event that compromises, or has the potential to compromise, the confidentiality, integrity or availability of APAC information or systems, including cyber security incidents and privacy breaches involving personal information. Incidents must be identified, reported, assessed, contained, investigated and remediated in accordance with approved procedures. Where an incident involves personal information, APAC must assess whether it constitutes an eligible data breach and respond in accordance with the Privacy Act 1988 (Cth), the Notifiable Data Breaches scheme and APAC's Privacy Policy and Procedure
- Incidents and privacy breaches must be managed in accordance with APAC's approved incident, critical incident, privacy breach and business continuity arrangements, as applicable. Business continuity and disaster recovery procedures may be invoked where service disruption is material
- Cyber security events, suspected security weaknesses, and actual or suspected privacy breaches must be reported immediately to the GEDU group (parent organisation) IT Team / APAC nominated IT contact and escalated in accordance with the approved incident reporting and breach response process.

Where an incident has broader operational, student welfare, safety, regulatory or reputational implications, it must also be escalated and managed in coordination with APAC's Critical Incident Management Policy and Procedure.

Cyber Security Governance and Oversight

Cyber security governance forms part of APAC's overall governance, risk management and compliance framework.

APAC will maintain a cyber security governance framework that ensures accountability, oversight, enterprise risk management and continual improvement of information security capabilities.

Governance activities include:

- Oversight by the Board of Directors through the Finance, Audit and Risk Management (FARM) Committee.
- Integration of cyber security risks into APAC's enterprise risk management processes.
- Review of cyber security risks and control effectiveness at least annually and following material incidents, significant technology or organisational changes, major supplier changes or relevant regulatory developments.
- Monitoring compliance with information security policies, standards and procedures.
- Monitoring third-party cyber security risks and supplier assurance activities.
- Independent internal or external reviews of cyber security controls where appropriate
- Findings from audits, assessments and assurance activities must be assigned to accountable owners, prioritised according to risk and tracked through to verified closure.
- Review of cyber security metrics and remediation activities.
- Consideration of cyber security requirements during major projects, technology implementations, supplier onboarding and significant organisational changes.
- Regular testing of incident response, backup recovery and business continuity arrangements.
- Ongoing alignment with recognised frameworks including the ACSC Essential Eight, relevant ISO 27001 control domains and applicable GEDU standards.

APAC Management and GEDU Group IT will provide periodic reporting to the FARM Committee covering:

- Significant cyber security risks and remediation activities.
- Material incidents and lessons learned.
- Essential Eight maturity improvement activities.
- Results of privileged account and user access reviews.
- Information security awareness and training metrics.

- Vulnerability management performance.
- Third-party security assessments and remediation activities.
- Material AI governance risks and mitigation activities.

Information Security Roles and Responsibilities

- Information security is the responsibility of everyone to understand and adhere to the policies, follow processes and report suspected or actual breaches.

Responsibilities of All Users

Users are responsible for:

- Cyber Security Events or breaches of security controls must be reported to the GEDU Group IT team immediately, even if only suspected.
- Use of all remote desktop software presents a significant threat to the security of APAC's Digital Services. As such, the CEO and GEDU Group IT team must first authorise and approve any software solution that provides remote access, to ensure the confidentiality, integrity, and availability of APAC's Digital Services and Data.
- When using or accessing APAC Digital Services remotely or from a personal device, be aware of the inherent risks to the privacy of confidential and sensitive information kept in those services and ensure the personal device used to access APAC's Digital Services is up-to-date and virus free and will not circumvent or compromise the security controls the institution places around its Digital Services.
- Keep passwords confidential and do not disclose them to others.
- Change their password as soon as possible if they suspect, or come to know, that their password has been compromised.
- Distribute, transmit, move, or delete information assets only if there is a valid business or academic need to do so.
- Not remove APAC information assets or equipment from APAC facilities without prior authorisation. An authorisation is deemed to have been granted to use APAC-issued portable devices (such as laptops, mobiles, and tablets), to conduct daily business activities from remote locations.
- Distribute, transmit, move, or delete information assets in accordance with APAC information handling standards and relevant contractual regulations and legal regulations.
- Users must not store APAC confidential, restricted, student, staff, financial, health or other sensitive information on unapproved third-party services, personal cloud storage, or unauthorised AI, collaboration or file-sharing platforms. Storage or processing on approved providers must be authorised, risk-assessed, and subject to contractual, privacy and security controls

Responsibilities of APAC

APAC executive management, with operational support from GEDU Group (parent organisation) IT and approved service providers, is responsible for:

- To establish the Digital Information Security Policy, defining, and supporting a strong security culture.
- Through the Finance, Audit and Risk Management Committee (FARM) ensuring the APAC has effective cyber security and foreign interference controls in place to protect the Company.
- The review of digital material which can pose a risk to the APAC is undertaken by appropriate Marketing and Communications authorised personnel.
- Supporting implementation and oversight of the Information Security Awareness, Training and Compliance Programme.

Responsibilities of the APAC Management Team

APAC Management Team is responsible for:

- Authorising the appropriate group(s) within GEDU Group IT to perform specific procedures for ensuring APAC's Cyber Security, including those identified within this policy.
- All Cyber Security Events reported to GEDU Group IT are evaluated to determine if a response is required. If a response is required, the Event becomes a Cyber Security Incident and will be managed by the appropriate response team. This will ensure a consistent and effective approach to the management of Cyber Security Incidents, including communications, and that the collection and analysis of evidence from the Cyber Security Incident occurs without compromising its integrity.
- Logs are reviewed to identify and manage Cyber Security Incidents and/or breaches in the security of Digital Services, as well as create and manage records and documents associated with Cyber Security Incidents for further analysis. In the event of a breach in APAC's Information Security, GEDU Group IT will triage the event and notify appropriate parties within APAC if personal data is involved.
- Controls and other preventative measures are put in place to avoid Cyber Security Incidents, either because of experience from previous Cyber Security Incidents or as a countermeasure or deterrent to likely Cyber Security Incidents. These measures are documented and regularly reviewed to ensure their validity and reliability.
- If a Cyber Security Incident is identified as originating from a state-based foreign act or, escalation within and external to the APAC is considered appropriate in the interests of national security.

Responsibilities of the CEO, APAC Management and Head of IT/ Delegated GEDU Group IT Service Leads

The CEO, APAC Management and Head of IT/ Delegated GEDU Group IT Service Leads are responsible for:

- Actively supporting information security through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
- Ensuring that all information security roles and responsibilities are clearly allocated.
- Ensuring that the Information Security Policy and all supporting processes are effectively implemented in their areas of responsibility.
- Conducting risk assessments to identify and define the positions that require applicants to pass personal background checks as part of the recruitment process; and
- Communicating to staff members leaving APAC their ongoing responsibilities to APAC (which include ongoing confidentiality requirements in relation to APAC's information assets).

Responsibilities of Asset and Service Owners

Asset and Service Owners are responsible for:

- Ensuring that all visitors and contractors are given temporary authorisation for appropriate system access, which will expire on the visitor or contractor's expected departure date or contract end date.
- Security Controls being implemented and maintained according to the relevant APAC security standards.
- The confidentiality, integrity and availability of information assets and information systems is protected by appropriate controls that are determined through a risk-based approach.
- Asset and service owners must maintain an inventory of assets under their responsibility, ensure classification of information, approve access based on least privilege, and participate in risk, supplier, backup and recovery planning for those assets and services.
- Asset and Service Owners must review and formally certify user access permissions for systems under their responsibility at least every six months to ensure access remains appropriate, authorised, aligned to business need and consistent with least privilege principles. Identified access issues must be documented and remediated within an appropriate timeframe.

Responsibilities of External Providers

- External providers must not commence handling or processing any information assets for the APAC until it has entered an appropriate contract with APAC that includes relevant information security controls with which the provider must comply.
- Without limiting external providers' other obligations, external providers must implement, operate and maintain the information security, privacy, breach notification, access control,

continuity, audit and exit / data return or destruction controls specified in their contracts with APAC

- The GEDU Group IT will monitor and review external provider services and manage any changes to external provider contracts considering information assets and information systems.
- External providers must ensure that they only connect devices to APAC network using approved secure access methods.

Monitoring

- Compliance with this Policy and the supporting information security management system will be monitored through management oversight, access reviews, incident metrics, vulnerability and patch reporting, backup test results, internal audit activities, and external assurance or audit where applicable.

Legal and Regulatory Obligations

- APAC takes its legal and regulatory obligations seriously and these requirements are documented.

Information Security Awareness, Training and Compliance

APAC will maintain a formal Information Security Awareness, Training and Compliance Programme to ensure staff, contractors, consultants and other authorised users understand and fulfil their information security responsibilities.

The programme will include:

- Mandatory cyber and information security awareness training during onboarding.
- Mandatory annual refresher training.
- Role-based training for personnel with privileged access, responsibility for sensitive information, system administration or information security responsibilities.
- Where required by risk, applicable role-based training must be completed before privileged access or access to Restricted information is granted.
- Security awareness content covering cyber security threats, privacy obligations, phishing, ransomware, social engineering, acceptable use requirements, information handling obligations and AI-related risks.
- Periodic phishing simulation exercises, security awareness campaigns and targeted retraining.
- Additional training following significant cyber incidents, material technology changes, major control failures or regulatory changes.
- Monitoring and reporting of training completion rates, overdue training, phishing simulation outcomes and targeted remediation to APAC Management and relevant governance bodies.

Managers are responsible for ensuring personnel complete mandatory training within required timeframes.

Training completion records must be retained for governance, compliance and audit purposes.

Third parties with access to APAC systems or Confidential or Restricted information must complete applicable APAC awareness training or demonstrate equivalent training appropriate to their access and responsibilities.

Failure to complete mandatory information security training may result in management escalation and restriction or suspension of access to APAC systems until training obligations are met.

Third parties with access to APAC systems or Confidential or Restricted information must complete applicable APAC awareness training or demonstrate equivalent training appropriate to their access and responsibilities.

Failure to complete mandatory information security training may result in management escalation and restriction or suspension of access to APAC systems until training obligations are met.

Continual Improvement of the Management System

- The information security management system is continually improved and documented to ensure that there is a continual improvement process in place.

Policy Compliance

Compliance Measurement

The APAC management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Information Security Control Exceptions

Where compliance with this Policy or a supporting security control is not technically, legally or operationally feasible, a documented exception must be formally approved before the non-compliant activity begins.

The exception must include:

- Business justification.
- Affected information, systems or services.
- Identified risks.
- Compensating controls.
- Assigned risk owner.
- Approval authority.
- Approval period and expiry date.

Australian Performing Arts Conservatory ABN 11 009 772 481
Registered as an Australian Institution of Higher Education PRV14046 CRICOS Provider Number 03897G

- Review or remediation date.

Exceptions must be approved by the relevant APAC business or Information Owner and GEDU Group IT or its delegated security authority. High or critical residual-risk exceptions must be escalated to the Chief Executive Officer and FARM Committee. Approved exceptions must be periodically reviewed and closed when no longer required.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.

Australian Performing Arts Conservatory ABN 11 009 772 481
Registered as an Australian Institution of Higher Education PRV14046 CRICOS Provider Number 03897G

Version Control and Document Owner

Policy Category	Operational	**Approval Date**	2 November 2026
Document Owner	Chief Executive Officer	**Approval Authority**	The Board of Directors
Audience	Staff	**Review Date**	November 2029

Revision History

Version	Author	Change Summary	Date Approved	Date Effective
1.0	DVE Business Solutions Pty Ltd	New document.	9 December 2022	
1.1	APAC	Review and update of policy and procedure.	25 January 2023	
1.2	DVE Business Solutions Pty Ltd	Added education agents to scope. Approved by Document Owner.	24 May 2023	24 May 2023
1.3	APAC	Change from QRMC to FARM Committee		22 May 2024
2.0	APAC	Change to document format. Update to GEDU Group IT references. Change title to 'Cyber and Information Security Policy'. Additions provided by GEDU Group IT.	2 November 2026	2 November 2026

Australian Performing Arts Conservatory ABN 11 009 772 481
Registered as an Australian Institution of Higher Education PRV14046 CRICOS Provider Number 03897G