Information and communications technology (ICT) security policy

**Acknowledgement**

The Victorian Curriculum and Assessment Authority proudly acknowledges and pays respect to Victoria’s Aboriginal and Torres Strait Islander communities and their rich and enduring cultures.

We acknowledge Aboriginal and Torres Strait Islander people as Australia’s first peoples and as the Traditional Owners and custodians of the lands and waters on which we rely. We pay respect to Elders past and present of the lands where we conduct our work and recognise their ongoing contributions as the first educators on the land now known as Victoria.

Authorised and published by the Victorian Curriculum and Assessment Authority
Level 7, 200 Victoria Parade
East Melbourne VIC 3002

© Victorian Curriculum and Assessment Authority 2024

No part of this publication may be reproduced except as specified under the *Copyright Act 1968* or by permission from the VCAA. Excepting third-party elements, schools may use this resource in accordance with the [VCAA educational allowance](https://www.vcaa.vic.edu.au/Footer/Pages/Copyright.aspx). For more information go to <https://www.vcaa.vic.edu.au/Footer/Pages/Copyright.aspx>.

The VCAA provides the only official, up-to-date versions of VCAA publications. Details of updates can be found on the VCAA website at [www.vcaa.vic.edu.au](https://www.vcaa.vic.edu.au/Pages/HomePage.aspx).

This publication may contain copyright material belonging to a third party. Every effort has been made to contact all copyright owners. If you believe that material in this publication is an infringement of your copyright, please email the Copyright Officer vcaa.copyright@edumail.vic.gov.au

Copyright in materials appearing at any sites linked to this document rests with the copyright owner/s of those materials, subject to the Copyright Act. The VCAA recommends you refer to copyright statements at linked sites before using such materials.

The VCAA logo is a registered trademark of the Victorian Curriculum and Assessment Authority.

|  |
| --- |
| Contact us if you need this information in an accessible format, for example, large print or audio.Telephone (03) 9032 1635 or email vcaa.publications@education.vic.gov.au |

Contents

[1. Overview 2](#_Toc178074591)

[2. Objectives 2](#_Toc178074592)

[3. Principles 2](#_Toc178074593)

[3.1 Clear responsibility and accountability 2](#_Toc178074594)

[3.2 Security management 2](#_Toc178074595)

[3.3 Resource identification and management 2](#_Toc178074596)

[3.4 Preventative measures and incident response 2](#_Toc178074597)

[4. Roles and responsibilities 3](#_Toc178074610)

[4.1 Executive directors, managers and authorised delegates 3](#_Toc178074611)

[4.2 Employees 3](#_Toc178074612)

[5. Expectations 3](#_Toc178074613)

[5.1 Effective information security management 3](#_Toc178074614)

[5.2 Communications and operations management 3](#_Toc178074615)

[5.3 Physical and environmental security 4](#_Toc178074616)

[5.4 Human resources security 4](#_Toc178074617)

[5.5 Business continuity management 4](#_Toc178074618)

[5.6 Information systems acquisition, development and maintenance 4](#_Toc178074619)

[5.7 Access control 4](#_Toc178074620)

[5.8 Compliance 4](#_Toc178074621)

[5.9 VCAA-specific compliance 4](#_Toc178074622)

[5.10 Privacy and human rights 5](#_Toc178074623)

[5.11 Further assistance 5](#_Toc178074624)

[5.12 Definitions 5](#_Toc178074625)

[6. Managing this policy 5](#_Toc178074626)

[6.1 Authorisation 5](#_Toc178074627)

[6.2 Accountability for the policy 5](#_Toc178074628)

[6.3 Important dates 5](#_Toc178074629)

[7. Related documents 5](#_Toc178074630)

1. Overview

The Information and Communications Technology (ICT) security policy serves to communicate the Victorian Curriculum and Assessment Authority's (VCAA) expectations for staff in relation to standards in ICT security. This policy establishes a framework aimed at safeguarding the integrity, confidentiality, and accessibility of sensitive information. The outlined security measures within this policy are instrumental in ensuring:

* the confidentiality and protection of sensitive information from unauthorised access or disclosure
* that information is accurate and complete
* ICT is available when required.

This policy applies to all employees within the VCAA. For the purposes of this policy, the term ‘employees’ encompasses employees directly employed by the VCAA, as well as any individuals or groups undertaking an activity for or on behalf of the VCAA, including:

* all employees (fixed term, casual, sessional) employed under Ministerial Order No. 1451 – Victorian Curriculum and Assessment Authority employees (Employment Conditions, Salaries, Allowances, Selection and Conduct) Order 2023 (referred to as ‘The MO’)
* volunteers
* Board members
1. Objectives
* **Universal access security:** ensure that all employees, regardless of their work location, adhere to security protocols when accessing a wide range of ICT resources, including LANs, WANs, WLANs, email systems, computer systems, and various devices
* **Comprehensive resource protection**: establish security measures that cover a diverse spectrum of ICT assets, including servers, desktops, printers, scanners, portable computers, mobile phones, storage devices, and handheld gadgets, to mitigate potential vulnerabilities across the technology landscape
* **Consistent security standards:** enforce uniform security standards and protocols across all ICT resources and devices, maintaining a cohesive and comprehensive approach to safeguarding data and systems
* **Risk mitigation for varied devices:** implement measures to mitigate security risks associated with a wide array of devices, ranging from traditional computers to portable devices like laptops, mobile phones, cameras, USB sticks and smartphones.
1. Principles
	1. Clear responsibility and accountability

Establish clear roles and responsibilities for all employees with authorised access to ICT resources, including VCAA's commitment to addressing legal, regulatory, and contractual requirements.

* 1. Security management

Implement a holistic approach to information security management involving coordination across different organisational segments, regular independent reviews, and continuous improvement to address evolving threats.

* 1. Resource identification and management

Identify, classify, and manage ICT assets effectively, including information, equipment, and software, ensuring proper ownership, acceptable use policies, and secure disposal procedures.

* 1. Preventative measures and incident response

Proactively prevent unauthorised access or breaches through robust access controls, physical and environmental security measures, while also establishing clear incident response protocols for timely resolution of security incidents.

1. Roles and responsibilities
	1. Executive directors, managers and authorised delegates

Executive directors, managers and [authorised delegates](https://www.vcaa.vic.edu.au/Documents/workwithus/HR/VCAADelegationsFramework.docx) are responsible for:

* ensuring the policy is effectively communicated to all employees
* ensuring that information security measures align with the value of assets and associated threats
* addressing and staying informed about legal, regulatory, and contractual requirements related to information assets
* reviewing and managing access levels required for employees.
	1. Employees

Employees are responsible for:

* adhering strictly to the ICT security policy, relevant procedures and associated best practices when using and accessing ICT resources
* promptly reporting observed or suspected security weaknesses or incidents in ICT systems or services to VCAA vcaa.servicedesk@education.vic.gov.au or 7022 5700
* promptly reporting any suspected or confirmed breaches of this policy and associated procedures to vcaa.servicedesk@education.vic.gov.au or 7022 5700
* ensuring responsible and secure handling of ICT assets, including portable devices, storage media, and equipment, especially when used outside VCAA premises.
1. Expectations
	1. Effective information security management
* management's active support through clear direction, commitment, and explicit assignment of security responsibilities
* coordination of security activities across the organisation by representatives with relevant roles
* clear definition of all information security responsibilities
* regular review of confidentiality/non-disclosure agreements reflecting VCAA's information protection needs
* maintenance of contacts with relevant authorities, security forums, and professional associations
* regular independent review of information security management approach and implementation
* security of VCAA information with external parties.

Maintain the security of VCAA information and processing facilities that are accessed or managed by external parties using the following practices:

* identify risks from external business processes and implement appropriate controls
* identify and address security requirements before granting external user access
* ensure agreements with external parties cover all relevant security requirements for accessing VCAA information or processing facilities.
	1. Communications and operations management
* To ensure stable and resilient operation of the VCAA's ICT network, responsibilities and procedures for operating management will be maintained, including the management of changes, third parties, backups and security operations. This will include:
	+ correct and secure operation of information processing facilities
	+ maintaining security and service delivery with external parties
	+ minimising system failures
	+ maintaining integrity and availability of software and information
	+ secure disposal of media
	+ security in information exchange
	+ detection of unauthorised activities
	+ system clock synchronisation.
	1. Physical and environmental security
* the VCAA will maintain an inventory that identifies all VCAA information and assets considered important, and assign a designated owner for all information and assets
* the VCAA will ensure locations that contain VCAA information assets will be protected from unauthorised access by the use of secure areas and that the impact of loss, damage, theft or compromise of assets will be minimised by protecting VCAA information assets
* define and implement rules for the acceptable use of information and related assets
* classify information based on value, legal requirements, sensitivity, and criticality to the VCAA
* develop and implement procedures for information labelling and handling aligned with the VCAA's classification scheme.
	1. Human resources security

All employees may be required to undergo pre-employment checks, be informed of their responsibilities for information security, undergo recurring security awareness training and, if appropriate, have their access to VCAA information assets removed upon termination of employment or change of roles.

* 1. Business continuity management

Business continuity plans for the VCAA will specifically address the need to continue to secure VCAA information assets in the event of a disruption to normal business.

* 1. Information systems acquisition, development and maintenance

Business requirements will include security considerations for new and existing information systems.

* 1. Access control
* each account will be uniquely attributable to an individual who will be held accountable for its activity
* access to VCAA information and assets will be supported by a legitimate business requirement
* network, operating system and application controls will prevent unauthorised access; this will include using secure log-on procedures, quality password management systems and unique User Id for each employee.
	1. Compliance
* VCAA information and assets will be managed to ensure progressive compliance with legal (for example, statutory, regulatory and contractual) requirements, along with VCAA policies and standards
* compliance checking will measure progress on a regular basis.
	1. VCAA-specific compliance
* **managerial oversight:** managers to ensure correct execution of security procedures for compliance
* **regular compliance checks:** regularly check information systems to ensure compliance with security implementation standards
* **Security testing protocol:** perform security tests on critical applications annually and after significant incidents or changes.
	1. Privacy and human rights

**Legislative compliance:** the policy aligns with the stipulations of the *Information Privacy Act 2000* (Vic) and the *Privacy and Data Protection Act 2014* (Vic), as well as *Charter of Human Rights and Responsibilities Act 2006* (Vic).

* 1. Further assistance

Employees can direct queries about this policy to the VCAA Information Technology Unit Manager.

* 1. Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| ICT | Information and Communications Technology |
| VPDSS | Victorian Protective Data Security Standards |

1. Managing this policy
	1. Authorisation

This policy is issued under the authority of the Chief Executive Officer.

* 1. Accountability for the policy

The owner for this policy is VCAA Human Resources. The owner reports to the Chief Executive Officer on the management of this policy.

The owner is responsible for:

* development and regular review of this policy
* development of protocols, processes and guidelines to support implementation
* monitoring compliance of applicable employees, organisational units, and/or locations.
	1. Important dates

|  |  |
| --- | --- |
| Date of adoption: | July 2024 |
| Date of last amendment: | July 2024 |
| Date of next review: | July 2026 |

1. Related documents
* *Information Privacy Act 2000*
* *Privacy and Data Protection Act 2014*
* *Charter of Human Rights and Responsibilities Act 2006*