Information Security Policy

Help for non-English speakers
If you need help to understand the information in this policy, please contact Templeton Primary School on 03 9801 7450 or templeton.ps@education.vic.gov.au.

Policy

This policy supports schools to manage and share information appropriately and securely to meet all protective data security requirements to protect staff, student and family information.

Summary

Schools must:

- assess and document information security risks including the effectiveness of controls, once per term in the pre-populated Information security school risk register in accordance with the Risk Management – Schools policy
- include information security controls in emergency management and disaster recovery practices
- implement information access controls (for example, access to school systems, key management, swipe card access, visitor processes) and review at least once per term to ensure that access is appropriately authorised and updated to only those who need information for their role
- encourage staff to complete information security awareness training upon engagement and repeat annually thereafter (available on LearnED)
- immediately report all potential or confirmed information security incidents to the department using the processes outlined in the Managing and Reporting School Incidents (Including Emergencies) policy
- when engaging third parties, ensure they securely manage school information and return or delete this information when it is no longer needed, in accordance with the Records Management policy

- complete annual information security reports required by the department. Schools will be advised when they will be included in the department’s annual reporting program as part of their transition to using department-provided technologies
- conduct pre-employment screening and ongoing eligibility checks for staff, volunteers and contractors
- ensure all school ICT assets are tracked and managed across their lifecycle
- implement and maintain physical security measures to protect school information and school ICT equipment and systems, both within and outside school premises. This includes the maintenance, repairs and secure disposal of ICT equipment, door locks, secure storage, bins and filing cabinets.

The Guidance tab provides advice to schools on the information security controls they are required to implement.

Details

The consequences of an information security breach can be far-reaching and potentially affect staff, students, families, school reputation, and confidence in the education system.

Schools must protect and share information in accordance with department information security policies and guidelines, which align with Victorian Protective Data Security Standards (VPDSS), published by the Office of the Victorian Information Commissioner (OVIC).

Schools must implement control measures to protect the confidentiality, integrity and availability of school information and the safety of their staff, students, and the community. These controls include 5 key security areas: Governance, Information, Personnel, Information and Communication Technology (ICT), and Physical.
By implementing the security controls outlined in the Guidance tab, schools can effectively protect school information and maintain a secure education environment in support of Child Safe Standards.

Available support

To report cyber security incidents:

- call the Incident Support and Operations Centre (ISOC) on 1800 126 126 to log an incident and request department support
- log a ticket on the Services Portal

For enquiries about the VPDSS reporting process:

- call: 03 7022 0002
- email: vpdss.attestation@education.vic.gov.au

Definitions

Centrally attested school
A school that has transitioned to department-provided ICT services and platforms to enable the department to attest on their behalf for the majority of VPDSS controls. Centrally attested schools complete a streamlined annual information security compliance activity as part of the department's central attestation process. By 2028, all Victorian government schools will transition to this reporting process and will be considered centrally attested schools.

Cyber security incident
An unwanted or unexpected cyber security event, or a series of such events, that has either compromised school operations or has a significant probability of compromising school operations. Cyber security incidents are considered information security incidents.

Contracted service provider
A person or organisation (public or private) that provides services under a contract. These may also be referred to as outsourced service or third-party providers.

Controls
Measures that schools use to maintain the confidentiality, integrity and availability of school ICT systems. The strength of the controls applied to a particular document or ICT system depends on the consequences of that document or ICT system being compromised.

Information security
The protection of school information through systematic application of controls (procedural, physical and personnel) to protect the confidentiality, integrity and availability of school information from a diverse range of threats from bushfires to sophisticated hackers.

Information security incident
An information security incident is any event that compromises the confidentiality, integrity, or availability of school information or school ICT systems. This can include:

- unauthorised access to school information
- data loss from both external and internal threats
- computer viruses or ransomware attacks (malicious software)
- improper sharing, accidental disclosure or changing of data.

School assets
Physical and digital resources that process, store, or transmit school information in any form. This includes workstations, filing cabinets, storage facilities, network devices and removable media.

School ICT systems
The integrated hardware, software, and network infrastructure used to securely process and store school information while maintaining confidentiality, integrity, and availability.

School information
Any information that schools create, collect, store, or use to support school operations and teaching activities. This includes digital records (such as emails, websites and electronic documents) and physical records (such as paper files and printed materials), managed by schools or third parties. While all school information must be protected, not all information is considered sensitive information – for example, publicly available timetables versus confidential student records. School information can also be referred to as school data.

Personnel security
The process of managing staff, volunteers, and third parties' access to information and school ICT systems across the following phases:

- pre-engagement checks for suitability and eligibility before hiring
- ongoing monitoring during employment and re-engagement
- off-boarding procedures when someone separates from the school.

Physical security
Physical protection controls designed to prevent unauthorised access or compromise of school ICT systems and school assets. Includes securing critical ICT systems, equipment, and planning for emergencies.

Sensitive information
A subset of all school information that, if compromised, could potentially cause adverse effects on school operations, assets, staff, students, families and community safety. Access to sensitive information should be limited to authorised persons based on the information needed for their role.

Sensitive information for this policy and guidance in schools includes, but is not limited to the following:

- student data, including name, address and date of birth
- student academic records, progress reports, assignments and assessments
- student health and medication information
- student information pertaining to family circumstances, including Intervention Orders and Family Court decisions
- student class photographs and individual images
- parents' names, address, phone number, email address and custody instructions
- teachers' personal information
- parents' banking and credit card information (including hard-copy records)
- school financial information
- tendering and procurement documents
- vendor invoices, contracts, accounts payable and receivables.

Note: The use of the term 'sensitive information' in this Information Security policy is distinct from the definition of 'sensitive information' as defined in the Privacy and Data Protection Act 2014 (Vic). Refer to the Privacy and Information Sharing policy for a definition of 'sensitive information' from a privacy perspective, as regulated by Part 3 of the Privacy and Data Protection Act 2014.

Related policies

- Acceptable Use Policy for ICT Resources
- Child Safe Standards
- Crime Prevention in Schools
- CCTV in Schools – Installation and Management
- Digital Learning
- Digital Technologies – Responsible Use
- Emergency and Critical Incident Management Planning
- Finance Manual – Financial Management for Schools
- Generative Artificial Intelligence
- Managing and Reporting School Incidents (Including Emergencies)
- Philanthropic Partnerships
- Privacy and Information Sharing
- Procurement – Schools
- Records Management
- Records Management – Employee Information
- Recruitment in Schools
- Requests for Information about Students
- Risk Management – Schools
- Software and Administration Systems
- Suitability for Employment Checks
- Sponsorship
- Technologies and ICT Services
- Visitors in Schools
- Volunteers in Schools
- Working with Children Checks and Other Suitability Checks for School Volunteers and Visitors

Relevant standards

- Victorian Protective Data Security Standards (VPDSS)

Relevant legislation

- Child Wellbeing and Safety Act 2005 (Vic)
- Copyright Act 1968 (Cth)

- Education Training and Reform Act 2006 (Vic)
- Electronic Transaction Act 2000 (Vic)
- Evidence Act 2008 (Vic)
- Financial Management Act 1994 (Vic)
- Freedom of Information Act 1982 (Vic)
- Health Records Act 2001 (Vic)
- Privacy and Data Protection Act 2014 (Vic)
- Public Administration Act 2004 (Vic)
- Public Records Act 1973 (Vic)
- Victorian Data Sharing Act 2017 (Vic)

Policy Review and Approval

Policy last reviewed	May 2025
Approved by	Principal
Next scheduled review date	May 2028