Software and Administration Systems

Policy

This policy defines the mandatory systems of record for student and school administration. It also outlines requirements for schools to use the Safer Technologies 4 Schools (ST4S) risk assessment reports for assessing both existing and new software and administration systems prior to use at a school.

Summary

- Schools must use the department-provided systems of record in accordance with their purpose and functions. If using administration systems not provided by the department, schools must ensure that any data used in these systems is exported into the relevant department-provided system of record.
- Prior to adopting new software or an administration system that is not provided by the department, schools must check if it has a Safer Technology 4 Schools (ST4S) assessment on the Arc Software catalogue and implement actions from the full ST4S report. If a report is not available schools must contact the department's IT Security team for alternative assessment options.
- For all currently used software and administration systems not provided by the department, schools must complete the required actions outlined in this policy by the end of 2028.

Scope

This policy applies to any software or administration systems that interact with or process personally identifiable, sensitive, health or important operational data (for example, a student management system accessed through a personal mobile).

For software or administration systems which do not process such information, this policy does not apply.

Systems of record

Schools must use the department-provided systems of record to record and maintain data, information and records, according to each system's purpose and functions. A list of department-provided systems of record can be found in the Guidance tab.

Schools may procure and implement further administration systems which provide additional capabilities for student and school administration. Examples include online services for parents and carers, assessment or grading tools, financial services or banking services.

Where a school implements one or more administration systems that is not provided by the department, they must ensure that any data, information or records generated or maintained in these systems is exported into the relevant system of record.

Adopting software and administration systems not provided by the department

Schools must comply with the following requirements prior to adopting (that is, purchasing, subscribing, trialling or renewing) software and administration systems not provided by the department).

Check Arc Software Catalogue

Prior to adopting new software or an administration system that is not provided by the department, schools must first check if it is listed on the Arc Software catalogue and whether it has a Safer Technology for Schools (ST4S) risk assessment report.

Arc Software can be filtered by the school-procured category and further filtered by functionality or learning area/capability tags (Products that are provided by the department are listed on Arc as 'Department provided' which will not have an ST4S assessment and are covered in the 'Department-provided software' guidance tab).

Use Safer Technology 4 Schools assessments

Where a Safer Technology 4 Schools (ST4S) report is available, schools must review the summary ST4S risk assessment report and implement actions from the full ST4S report prior to using the software or administration system.

Schools must not use products with an overall ST4S rating of non-compliant, non-participating or high risk. Refer to the Guidance tab for more information about ST4S assessments.

Request security assessments

Where an ST4S report is not available schools are encouraged to:

- search for alternative products that have been assessed which offer similar functionality as these represent a lower risk than unassessed products
- complete a privacy impact assessment (PIA). (Refer to guidance on privacy impact assessments within the Privacy and Information Sharing policy for more information).

Prior to using products which have not been fully assessed (as suitable alternative products may not always be available), schools must raise an assessment request with the department's IT Security Team via the Service Desk (staff login required) who will arrange for either an ST4S or other assessment to be conducted.

- Schools can use these products while this assessment is underway.
- Schools that have registered product assessment requests will be notified of the results.
- Pending the outcome of these assessments, schools may need to move to lower risk alternative products.

Using department contract template

Schools are strongly encouraged to use a department contract template when using software and administration systems to ensure compliance with department requirements. For more information refer to the systems and applications section of the Records Management policy.

Reviewing currently used software and administration systems

For all currently used software and administration systems, not provided by the department, schools must complete the following actions by the end of 2028:

- record an inventory of all the products they use (template in Resources tab)
- review any available ST4S assessment reports for these products
- implement actions from the full ST4S assessment reports for these products as soon as practicable; either 12 months after review, or by the end of 2028, whichever comes first.

Actions based on the software of administration system's ST4S risk rating

Refer to the Guidance tab for more information about ST4S product risk ratings.

If a school identifies or becomes aware of products, not provided by the department, already in use in the school with an ST4S rating, they must take the following actions:

- for ratings of non-compliant or high risk, or an outcome of non-participating – schools must cease use of this product or migrate to a lower risk alternative as soon as practicable and within 12 months
- for ratings of medium risk, low risk, use with caution, or use responsibly – full ST4S assessment report actions are to be reviewed and implemented as soon as practicable; within 12 months or by the end of 2028, whichever comes first.

This timeline is aligned to the Technologies and ICT Services policy.

Definitions

Administration systems
Administration systems refer to digital technology-based systems and processes for collecting, maintaining and using records (including for students, staff, parents and others).

Safer Technologies 4 Schools
The Safer Technologies 4 Schools (ST4S) initiative is an independent national service administered by Education Services Australia that creates security, privacy and child safety reports for schools.

Software
The digital applications that support teaching, learning and other functions in a school, and which may complement administration systems and technologies and ICT services including: locally installed applications, web-based applications, websites, web browser extensions, collaboration platform add-ons.

Student and school administration
The processes and activities which enable the day to day running of a school. These include:
- school management – including finance and accounting, procurement, facilities and asset management, human resource management, risk management, and ancillary services
- student administration – including enrolments and transitions, attendance, student reporting and achievement, student and family profiles, health and wellbeing, events and consent).

Systems of record
The department-provided administration systems which are considered to contain data and records where the integrity, validity and security of this information is vital to deliver required reporting and school operational functions.

Technologies and ICT services
Technologies and ICT services refer to infrastructure and platforms that enable core school functions including: hardware, internet, network, cloud services, identity management, operating systems and collaboration platforms. Refer to Technologies and ICT Services.

Related policies

- CCTV in Schools – Installation and Management
- Child Safe Standards
- Digital Learning

- Digital Technologies – Responsible Use
- eduMail (employee email)
- Generative Artificial Intelligence
- Information Security
- Privacy and Information Sharing
- Records Management
- Schools' privacy policy
- Technologies and ICT Services

Relevant legislation

- Child Wellbeing and Safety Act 2005 (Vic)
- Freedom of Information Act 1982 (Vic)
- Health Records Act 2001 (Vic)
- Ministerial Order 1359 – Implementing the Child Safe Standards – Managing the risk of child abuse in schools (PDF)
- Privacy and Data Protection Act 2014 (Vic)
- Public Records Act 1973 (Vic)
- Victorian Protective Data Security Framework

Evaluation

This policy will be reviewed in accordance with the school's three-year review cycle.

Last ratified by School Council in May 2025