



Technologies & ICT Services

Policy

This policy outlines the requirement for schools to transition to department-provided technologies by the end of 2028 and the support available for schools implementing technologies and Information and Communications Technology (ICT) services.

Summary

- The department provides a suite of technologies and ICT services to schools.
- Where a school has previously adopted technology now provided by the department, schools must transition to the department technologies by the end of 2028.
- Schools must not:
 - implement the same technologies where the technology is provided by the department
 - adopt different technologies where the department technology provides the same service.
- Where the technology is not provided by the department, schools may continue to adopt and use those technologies in accordance with department child safety, privacy, records management, procurement, backup and recovery, and information security requirements.

Details

By the end of 2028 schools must migrate their school-managed technologies to department-provided technologies where available.

This is because it is no longer appropriate for schools to operate separate technology environments due to:

- cyber security incidents increasing in both sophistication and frequency, resulting in privacy breaches and extended outages
- challenges with risk mitigation and responding to incidents in a diverse technology landscape
- the increased risk of harm if technology is adopted without necessary privacy, security and child safety assessments (Standard 9 of the Child Safe Standards requires schools and the department to maintain the safety of children in an online environment)
- the challenges associated with managing long-term record retention requirements including records that must be kept beyond system life.

Department-provided technologies and ICT services

The department provides a suite of technologies and services to schools. These technologies are regularly assessed for compliance with the child safety, privacy and security standards.

Department-provided technologies include:

- high speed internet access with content filtering
- collaboration platforms including Microsoft 365 and Google Workspace for Education
- video conferencing services including WebEx
- enterprise grade WiFi
- single department managed identity for staff and students (eduPass)
- access department ICT systems through Secure Remote Access Service (SRAS) when working remotely
- single email address for staff and students
- cloud-based device management solution
- server endpoint detection and response
- asset vulnerability monitoring and reporting services
- security incident logging and monitoring
- notebooks for school staff.

The department provides a range of ICT support for schools including:

- Technical Support to Schools Program (TSSP)
- [ICT purchasing panels](#) (staff login required)
- [Arc Software](#).
-

For more information, refer to [ICT support for schools](#) in the guidance chapter.

Migrating to department-provided technologies and ICT services

The [Securing Connected Learners \(SCL\) Program](#) (staff login required) has been established to support schools to migrate to department-provided technologies by the end of 2028. Schools will have the opportunity to influence improvements to the technology and services the department provides and will be contacted to advise of the migration process.

If existing commercial agreements for equipment, services and software are due for renewal and sufficient notice is provided, the SCL Program may be able to facilitate an early transition providing a cost-avoidance opportunity for schools. Please use the [Contact us](#) page to notify the SCL Program of these arrangements.

Adopting other technologies and ICT services

Schools may continue to adopt and use technologies not provided by the department in accordance with department policies (below). These technologies may include:

- building sign-in and access systems
- printing management systems
- library systems
- specialist device management systems
- hardware such as printers, multifunction devices, projectors, hearing augmentation
- Internet of Things (IoT) devices
- curriculum-specific hardware such as STEM tools (3D printers), art tools.

When seeking to use technologies not provided by the department, schools must ensure they comply with department policies, including:

- the review and implementation of Safer Technology for Schools (ST4S) risk assessment reports, as outlined in the [Software and Administration Systems policy](#)
- managing privacy risks including conducting Privacy Impact Assessments, as outlined [Privacy and Information Sharing policy](#)
- the measures required to securely and appropriately manage and share information, as outlined in the [Information Security policy](#)

- the appropriate management of access to communication with individuals outside the school in online environments, as outlined in the [Digital Technologies – Responsible Use policy](#)
- record retention requirements as outlined in the [Records Management policy](#).

Schools are strongly encouraged to use a department contract template when using technologies not provided by the department to ensure compliance with department requirements. For more information, refer to the [system and applications section of the Records Management policy](#).

In addition to the above requirements, schools, supported by TSSP personnel, must define, implement and support backup and recovery procedures for school ICT infrastructure to minimise IT security and business continuity risks associated with data loss. For more information, refer to [Backup and recovery of ICT infrastructure](#) in the guidance chapter.

Contact

Securing Connected Learners Program

SCLProgram@education.vic.gov.au

[Services Portal](#)

Phone number for schools: [1800 641 943](tel:1800641943)

Email: servicedesk@education.vic.gov.au

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) – refer to [Software and Administration Systems](#).

Internet of Things (IoT)

The physical objects that are connected to, and share data, with technologies and ICT services and software over the internet, including some: printers, multifunction devices, projectors, hearing augmentation devices, air filters, air conditioners, solar panel arrays, door locks, lights, security sensors, clocks.

Software

The digital applications that support teaching, learning and other functions in a school, and which complement Administration Systems and Technologies and ICT Services including: locally installed applications, web-based applications, websites, web browser extensions, collaboration platform add-ons – refer to [Software and Administration Systems](#).

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.

Related policies

- [Acceptable Use Policy for ICT Resources](#)
- [CCTV in Schools – Installation and Management](#)
- [Digital Learning](#)
- [Digital Technologies – Responsible Use](#)
- [eduMail \(employee email\)](#)
- [Information Security](#)
- [Notebooks for School Staff Program](#)
- [Privacy and Information Sharing](#)
- [Procurement – Schools](#)
- [Records Management](#)
- [Software and Administration Systems](#)

Relevant legislation

- [Child Wellbeing and Safety Act 2005 \(Vic\)](#)

- [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