NOVEMBER 2024

IT Infrastructure Plan 2024 to 2029

Department for Education,
Children and Young People

Tasmanian Government

Table of Contents

Version 1.0 – 10/11/2024

Strategic context for IT Infrastructure in DECYP

The Department of Education, Young People and Children (the department) has a complex state-wide network supporting over 58,102 desktops, laptops, and tablet devices at over 300 locations around the state.

The IT Infrastructure and Business Application Solutions and associated business processes enable staff and clients of the department to be able to transact their business in a secure and safe environment from any location at any time with a minimum of disruption.

To facilitate the vision, this plan aims to move the department's IT Infrastructure and Business Application Solutions from a centralised network environment to one that utilises a high bandwidth network (maximising the potential offered by fibre connections particularly under the NBN), allowing central and cloud storage of data and business application solutions that enable department owned or student and client owned devices secure access to the resources they require to enable them to carry out their business anywhere, anytime.

To better support the rollout and adoption of additional technology systems, this plan also encourages the development of technology governance processes that provide clear accountability on technology selection and prioritisation decisions and ensures that new technology is strategically aligned and provides value to the department. The governance framework is not meant to prohibit or slow down new technology requests, but rather provide a streamlined pipeline for the various consultation and technology review processes that need to occur.

In broad terms the strategic directions of this IT Infrastructure and Business Application Solutions plan provides for the following key business and technical elements:

- Scalability – the ability to handle growth and cater for a Bring Your Own Technology (BYOT) device model in the client (students, library users) areas.
- Consolidation – the ability to bring together existing IT infrastructure and business application solutions to provide a more efficient IT environment.
- Agility and versatility – the ability to respond to changing business requirements and the changing technology landscape.
- Empowerment – enable business and service areas to readily adopt technology in a way that suites their needs, in platforms that are secure, managed, and reliable.
- Security –to provide the protection required to individuals, data, and business application solutions, based on alignment with the Australian Cyber Security Centre's (ACSC) Essential Eight maturity model.
- Safe – provision of online environments that promote and support safety and wellbeing while minimising the opportunity for children and young people to be harmed.
- Monitor – the ability to monitor in real time, either directly or via vendors, all elements of IT infrastructure and business application solutions to ensure they are working effectively.
- Availability – the ability to provide IT services continuously.
- Provisioning – the ability to provide required IT resources in a timely manner to the right users.
- Business Continuity –to provide continuation of service in the event of an incident that impacts the delivery of that service, and the ability to recover from an unexpected event and protect the department's data and information.

Underpinning all these elements is the need to deliver this in the most cost-effective way. The IT Infrastructure and Business Application Solutions plan addresses these requirements and can be broken down into various IT infrastructure categories with Business Application Solutions as an additional category.

1 End User Infrastructure

1.1 Desktop computers, Laptops, and tablets

The department has over 58,640 desktop, laptop, and tablet devices, with over 50,000 of these located within schools including teacher laptops. The desktop operating system for desktop and laptop computers is currently Windows 11. iPads run on the Apple iOS operating system. Software updates for these are centrally controlled and are provisioned as shortly after release as possible, once testing has been completed in the department environment. These computing devices are covered by four-year onsite warranty, throughout Tasmania including the Bass Strait islands.

Strategic Direction

The department has streamlined its preferred suppliers for desktop, laptop and tablet computers being Lenovo, Microsoft and Apple This has allowed us to focus on providing the best support model for our devices. Providing quick turnaround times on device security updates, driver updates and feature enhancements improves the devices usability and security.

Over the past 12 months we have updated most of our staff devices through our Computers for Teachers program and our non-school's device refresh programs. In 2024 there will be the addition of approximately 2500 devices deployed to Teacher Assistants and other school-based support staff.

Over the past five years we have seen an increasing number of teachers adopting highly portable devices in preference to the more traditional larger format laptops. To assist in this classroom transformation, increased options for lightweight devices to be deployed to the classroom environment to complement the direction in which our teachers are moving.

The deployment of Windows 11 at scale as part of the Computers for Teachers device rollout allows our users to access a raft of new features and modern business tools. Updating school devices used by learners and office administration staff, as well as those used by non-school users allows all department users to be on the same platform which enhances collaborative working.

Replacement Cycle

The desktop, laptop and tablet computers are replaced in a four-to-five-year cycle.

The department supports a Bring Your Own Technology (BYOT) model for students on a school-by-school basis to cater for their local circumstances. BYOT is a supplementary service at the school to support a minimum of one school-owned computing device for every three students at the school.

Business and service delivery units (Corporate Sites) BCN 855	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	Totals
Facilities Management (1)	5	3	2	4	1	15
Non-school based staff	303	52	69	715	1,706	2,845
Libraries – staff	137	7	11	15	30	200
Libraries – Public Access	182	37	5	21	31	276
Total	**627**	**99**	**87**	**755**	**1,768**	**3,336**

School Sites BCN 823	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	Totals
Teachers Award (Computers for Teachers)	30	30	30	30	5,463	5,583
School Support Staff (2)	2,100	300	600	30	30	3,060
SBM / Admin Staff	0	0	680	0	0	680
Facilities Management (1)	68	19	33	17	8	145
Student Devices Year 11 and 12 Extension Schools	0	1,000	0	0	0	1,000
Student Loan Devices (Digital Inclusion Action Plan)	0	0	1,000	0	0	1,000
Total	**2,198**	**1,349**	**2,343**	**77**	**5,501**	**11,468**

School Sites (SRP Funded)	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	Totals
Student (3)	3,393	9,833	8,550	6,914	11,857	40,547
Total	**3,393**	**9,833**	**8,550**	**6,914**	**11,857**	**40,547**

Table 1 - End User Device replacement programs.

Note (1): Facilities Management device are devices that are not assigned to a staff member, that are provided by ITS and need to be replaced as part of our refresh cycle. They include such roles as:-

- Room controller, CCTV, building management, Telstra caching box

Note (2): Support staff is 3,000 staff members.

Note (3): Student devices are funded by individual schools via their SRP.

There are four device replacement programs that staff members can be assigned a device against, they are: -

- Non-school based staff – this covers all staff based in corporate offices, Libraries TAS, CFLC, ARL, etc.

For school-based staff there are three options

- Teacher award – all staff on the teacher award
- Admin staff – this includes SBM's and school admin staff
- Support staff – this includes teachers assistants

Staff should be assigned to one of these groups and allocated a device from within that pool. When staff have multiple roles, they will be assigned to the highest group they are a member of in the order of Teaching Staff – Admin staff – Support staff.

1.2 Software - Standard Operating Environment (SOE) managed by Intune

The desktop, laptop, and tablet standard operating environment SOE contains the base software installed on all desktop and laptop computers including Microsoft Windows operating system, Microsoft Endpoint Protection (anti virus / anti SPAM) and Microsoft 365 Office suite. The software licences for the SOE are coordinated and managed by ITS for all desktop, laptop and tablet computers owned by the department.

The device management for department devices, including Apple, was migrated to Microsoft Intune to modernise device management and standardise management of all operating systems in one platform.

Strategic Direction

Utilise an 'evergreen' release cycle where both feature and security updates are continuously released, optimising managing, updating, securing, and patching the operating system and SOE software applications.

- Optimisation of Intune Configuration: Fine-tune the configuration of Intune to align with the organisation's specific requirements and workflows. This includes setting up policies for security, application deployment, and compliance.
- Integration with existing systems: Integrate Intune with other existing systems and tools within the organisation's IT infrastructure to streamline processes and enhance efficiency. This could involve integrating with identity management systems, asset management tools, and service desk ticketing systems.

- Regular Monitoring and Maintenance: Improve monitoring strategy to ensure the smooth operation of Intune and department devices.
- Regularly review device compliance, security posture, and performance metrics to identify any issues or areas for improvement. We are looking at better ways to protect students using department devices on non-departmental networks this includes web filtering.

Replacement Cycle

Software is maintained, in most instances, in an evergreen state, with licences renewed yearly or as per their contract terms. Most software follows a regular (monthly, quarterly or annual) update patch cycle that both allows department staff to use the latest features as they are released as well as providing best practices for cyber security.

1.3 Printers and Multi-function devices

There are over 2100 printers of various makes and models located throughout the department including schools.

Over the past few years, the number of printers has dropped in schools and business units in favour of using multi-function devices (over 1000), which have print, scan and photocopy capability. These devices offer black and white and colour production. The department has preferred supplier(s) for multi-function devices being Ricoh and Konica Minolta.

To support a ‘follow me print’ function allowing employees to print at any location, the department utilises PaperCut MF software. There are currently two versions in use, a central cloud version and a local site version in some schools.

Where a multifunction device is not required a HP Desktop printer is utilised.

Strategic Direction

As business unit output requirements change or printers / multi-function devices require replacing, a review of the printer / copier requirements for the school and business area will be undertaken and from this a replacement strategy including replacement cycles will be developed for the individual school or business unit.

The preferences in developing this replacement strategy are:

- To lease, rather than purchase, multi-function devices.
- To minimise the use of desktop printers in favour of multi-function devices due to lower total cost of ownership.

To migrate all PaperCut local site versions from schools to the single central cloud version which will increase output options, while reduce management overhead of multiple versions and costs.

Replacement Cycle

Dependent on an individual school or business unit requirements as per their printer and multi-function device strategy. See the table below of current printer/multifunction device types.

Printers / Multi-Function Devices (Copiers)	HP	Ricoh	Konica Minolta	Other	Totals
Business and service delivery units	81	57	107	33	278
School	702	806	218	50	1,776

Table 2 – Printers and MFD types.

1.4 IT Support Costs

ITS has a mix of central IT staff and on-site IT staff. Central staff look after all central IT infrastructure located on-premises in the Government data centres, cloud hosted, and IT infrastructure distributed throughout business and service delivery units office and Library locations.

On site IT support in schools is allocated to schools on a ratio of the higher of department owned devices at the school or student FTE in the school, against the total state-wide IT school support staff number, with additional support provided by a central IT Helpdesk.

The IT Trainees located in schools are funded by the school via their annual School Resource Package, with all other IT Trainees positions supporting business and service delivery units locations funded in the central ITS budget.

2 Local Area Network

2.1 Local area network switches

Local Area Networks (LANs) are comprised of several distinct components - cabling (patch panels and communication cabinets), network devices (switches and wireless access points) and licensing. The department has standardised on Cisco for its networking hardware fleet. The licensing element of the network enables corresponding management solutions to be utilised to leverage return on investment and provide management of the equipment and other functionality (see 3.3 below).

Strategic Direction

Continuously review and update the department's Data Cabling Standards with the requirement that these must be referenced and adhered to for all building works and installations. ITS works closely with the department's Facility Services branch to ensure this occurs. All LAN cabling components must meet the department's Data Cabling Standards in all locations.

Asset data is collected and maintained as sites are upgraded, redeveloped, or built. Asset data reflects bandwidth, network devices, cabling specifications, racks, and other relevant configuration item (CI) information. All locations have Cisco network switches and wireless access points that support Whole of Government telephony services and identity-based access allowing both department and BYOT devices to be connected to the LAN.

- The Cisco network device fleet should remain current to avoid devices reaching end of vulnerability/security support periods thus enabling the deployment of scheduled software configuration updates to address vulnerabilities as they arise and maintain standard configuration across the networking equipment. Toolsets such as Cisco DNA-C can be utilised to manage and remediate the networking equipment in response to security vulnerabilities.
- Table 1 - End User Device replacement programs.
- Cisco networking equipment housed in the Government's Data Centres will be purchased with a Cisco 8x5x24 maintenance agreement for system failures. Failure of Cisco switches at all other sites will be addressed by either warranty or a backup supply of suitable spares.
- The Networking Tasmania LANaaS offering provides additional "value adds" or a catalogue of services in conjunction with the supply of networking equipment at Government shared office locations. This would consist of (but not be limited to) the availability of state-wide depots for the storage of switch hardware, pre-populating switches with modules and other components prior to deployment, delivery of switches to sites, storage of spares, hardware disposal, labelling of switches and provision of electronic serial numbers for switch hardware,.
- Continue to work with Telstra via the Networking Tasmania LANaaS agreement and Cisco on their new technology offerings, improvements, and network management toolsets with a view to evaluating these against business requirements and to assess technology stability within the department and Government network prior to wider deployment.

Replacement Cycle

LAN switches for business and service delivery units (Corporate) and School sites will be upgraded or replaced on a rolling 7-year cycle. This will be co-ordinated by IT Services. Licensing costs for operating systems should be included in the fleet renewal budget plan together with costs for ad hoc items (such as fibre modules) and planned minor cabling remediation works.

Business and service delivery units (Corporate Sites)	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	2029/30 Devices Replaced	2030/31 Devices Replaced	Totals
2.1 Local Area Network (LAN) Switches	21	12	39	69	29	14	10	194

School Sites	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	2029/30 Devices Replaced	2030/31 Devices Replaced	Totals
2.1 Local Area Network (LAN) Switches	261	270	239	204	234	243	249	1,700

Table 3 - LAN Hardware replaced on a rolling 7-year cycle.

2.2 Local Area Network cabling

The departments' Local Area Network (LAN) cabling is extensive and wide-ranging across many locations and buildings throughout the state. There is often a direct relationship between the age and condition of the building (or when it last had modifications) and the configuration and capacity of the cabling.

Strategic Direction

In conjunction with Facility Services and other parties, ITS have developed data cabling standards which are now included as requirements for all new building works.

The data cabling standards will be used as a reference point to ensure the LAN performs as expected and high-speed bandwidth is realised throughout the department's sites. The requirement for significant cabling or rack remediation works will be captured and provided to Facility Services based on remediation activities per site so that these can be included in the capital works budget. This will also include racks that require floor mounting to overcome potential safety and access issues.

Replacement Cycle

Cabling is reviewed and upgraded when building works are undertaken at the location and as part of remediation activities identified by ITS.

2.3 WIFI

The department's WIFI infrastructure is based on a Cisco solution provided by Telstra under the Networking Tasmania LANaaS agreement. This forms part of the whole of Tasmanian Government WIFI network enabling any Tasmanian public servant access from any location that has WIFI. This is largely managed by Telstra with level 1 support carried out by the department's IT support staff. The current fleet consists of over 5,800 Wireless Access Points (WAPs). To minimise client roaming issues at sites, locations are limited to a single model WAP wherever possible. Access to rich WIFI reporting and telemetry is limited in Telstra's shared environment with several portals providing WIFI information. Given this, most access points have now been transitioned to the

department's own DNAC platform so the benefits of richer telemetry data and reporting can be realised and a reduction in the number of management portals.

To date the criteria for the placement of WAPs has been one WAP per GLA (General Learning Area). In some cases, this has created problems, due to an oversaturation of WIFI resulting in excessive noise and interference. Additionally, it may not be the most cost-effective approach. WIFI site surveys should be undertaken as required to assist with optimal placement of WAPs as learning spaces and classrooms are re-designed and greenfield sites are established, or where sites report issues with WIFI coverage and throughput.

Strategic Direction

Regular review the availability of next generation WAPs and WIFI technology offered by Cisco including their Meraki WIFI products (e.g. 802.11ax and WIFI 6) with a view to continuously improving the end user experience. Current Cisco model WAPs offer compatibility with Meraki management systems which will provide future flexibility if the department chooses to move to a Meraki Cloud Management platform. To ensure optimum placement of WAPs in greenfield and redeveloped sites (and in locations where coverage issues are being experienced) site surveys will be conducted to determine optimum WAP placement and gain the best efficiencies from the WIFI fleet. Site surveys will also occur where sitewide WAP refreshes are taking place. To enable future migration to Software Defined Access (SDA) and realise a richer telemetry/reporting experience and improved operational management, the department has integrated its own DNA-C management portal instance.

The department's WAPs also support the new Whole of Government free public WIFI network in various corporate, Libraries Tasmania and other locations.

Replacement Cycle

WAPs for business and service delivery units, Corporate and School sites will be upgraded or replaced on a rolling 7year cycle. Licensing costs for operating systems should be included in the fleet renewal budget plan together with costs for associated required cabling as per the data cabling standards.

Business and service delivery units (Corporate Sites)	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	2029/30 Devices Replaced	2030/31 Devices Replaced	Totals
2.3 Local Area Network (LAN) WAP's	41	76	76	76	76	76	76	497

School Sites	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	2029/30 Devices Replaced	2030/31 Devices Replaced	Totals
2.3 Local Area Network (LAN) WAP's	1,024	719	719	719	719	719	719	5,338

Table 4 – Wifi Hardware replaced on a rolling 7year cycle

2.4 Network Monitoring, Management and Access

2.4.1 Network Management Tools, Network Access Control, and Internet Based Networking

Traditional network management toolsets are required to implement, manage, and control access to networks. Software defined access (SDA) now enables management, provisioning, and segmentation of the network fabric. In this context, access to the network is based on policy and identity rather than traditional Access Control Lists (ACLs) and Virtual Local Area Network (VLANs).

DNA-C (Digital Network Architecture Centre) and ISE (Identity Services Engine) are pre-requisites for SDA. DCNM (Data Centre Network Manager) is currently used to manage and monitor the Data Centre network switch fleet. Reporting and licensing is provided as part of Cisco hardware purchases.

Strategic Direction

Continue to consolidate Network management toolsets where possible and feasible. Work with DSS and Telstra in providing greater access, visibility and co-management options for government shared network management and monitoring systems. Evaluate new network management systems and technologies as they become available to assess their suitability for the department's network environment.

Undertake a review to establish and reconfirm the requirement for Software Defined Access (SDA) in light of technologies such as Direct Internet Access which shift network traffic directly to the internet.

Pending the outcome of the SDA review, conduct a proof of concept for SDA with the objective of removing the requirement for ACLs and VLANs. Access to the network is based on identity resulting in increased performance and security. It is anticipated that there would be ongoing costs associated with the procurement and ongoing licensing of Identity Services Engine (ISE) and this cost needs to be ascertained during the proof of concept.

Replacement Cycle

Implement upgrades or new network management systems and technologies as they become available.

2.4.2 Network Monitoring Tools and Logs

Monitoring toolsets including Security Information and Event Management (SIEM) solutions (e.g. Azure/Log Analytics) are used across the LAN, Data Centre and Wide Area Network environments. Appropriate toolsets can reduce management overheads significantly and leverage return on investment of existing network hardware infrastructure. They enable proactivity and an assurance that the network and related systems are operating optimally by providing increased visibility into the network. They also become increasingly important as on-premise Networks extend to the cloud.

Supporting toolsets can give visibility of communication between segments and applications, cyber threat intelligence feeds, baselines, indications of compromise, malware protection, logging, graphing, etc. Grafana is currently being used as a monitoring toolset. Log Analytics captures proxy logs, firewall logs, Netflow data, switch availability data and interface performance metrics. Many of these are critical log datasets from a regulatory and cybersecurity perspective.

Strategic Direction

The ongoing use of Azure/Log Analytics together with the centralisation of critical IT environment datasets should continue to form part of the department's strategic direction to facilitate single-pane-of-glass monitoring and reporting particularly as it relates to SIEM and cyber incident response. Other network monitoring solutions and management systems should continue to be evaluated as they become available to assess their suitability. These include toolsets which integrate with the department's Cisco technology fleet and provide monitoring and visibility of on-premise Networks extending to cloud performance including path visualisation.

Replacement Cycle

In most cases, toolsets such as Data Centre Network Manager (DCNM), are supplied as part of our yearly network switch and associated licensing purchases. Consideration should also be given to the purchase of additional toolsets not bundled with existing licensing, and particularly those toolsets which address existing gaps in functionality.

3 Wide Area Network

3.1 Wide Area Network

The department's Wide Area Network (WAN) is managed under the Whole of Government Networking Tasmania III contract. Under the contract, Telstra provide network core services including core switching, internet access, content filtering and inspection, load balancing, domain

name and IP address management, network authentication and authorisation, message gateway services and remote access services.

Telstra together with 42-24 and Field Services Group (FSG) provide approximately 330 connection services (WAN services) to the department under the contract. Department sites include schools, learning service and corporate offices, libraries, online access centres, child and family centres, youth justice and children and family services and shared (multi-department) sites. The three providers offer a range of WAN services including NBN enterprise and business grade services over various technologies. Network traffic at all department sites securely traverses the Network Core. Site connectivity, particularly at NBN fixed wireless sites, is complimented with a 4G failover service to provide a rudimentary level of redundancy.

Challenges continue to remain with limited-service offerings in remote locations throughout the State which often do not allow the use of higher speed fibre based connection services.

Internet access in the Network Core is provided by a 10 Gbps Telstra Internet Direct (TID) link dedicated solely for department use.

As WAN services are upgraded and speeds increase as they become available at locations throughout the state, congestion, and bottlenecks both at the local network level and within the network core are becoming increasingly common. This is particularly evident at times of high network usage which can be triggered by major events, e.g. Olympic Games.

Connectivity to resources hosted in Azure from on-premise is provided by a Microsoft ExpressRoute circuit provided by FSG.

Strategic Direction

In August 2022, DSS undertook a RFT seeking responses from vendors so that a new Data and Internet Services panel could be established and used by Tasmanian Government departments. Access to the new Data and Internet Services panel is now available (with Telstra services to be included by 3rd quarter 2024). New technologies include Low Earth Orbit (eg Starlink type) satellite services and discounted WAN services.

- Continue to work with DSS and network core and connection services panel providers to implement a Secure Access Service Edge (SASE) model incorporating SD-WAN technology to department sites. This will address WAN congestion at sites and within the Network core. It will also enable redundancy for sites by providing multiple WAN services and better visibility and control of network traffic ensuring WAN business continuity for essential business applications.
- Review and upgrade WAN services and technologies (e.g. Satellite technologies) to meet established minimum bandwidth requirements and provide an alternative to the sole reliance upon NBN Fixed Wireless. The increase in bandwidth capacity and options will also enable the adoption of a serverless IT infrastructure model in Schools removing IT infrastructure from the local site while improving service access.
- Continue to review network and cloud transit architecture (i.e. SD-WAN OnRamp and Azure Virtual WAN, etc). This can complement and/or reduce the reliance on the department's ExpressRoute service.

Replacement Cycle

The Networking Tasmania contract is broken down into several sub-parts covering the various elements of the WAN and internet access, with each of these sub-parts having different review / renewal periods. The department needs to maximise the benefits and flexibility offered by the Networking Tasmania contract and take advantage of rapid technology changes.

Review service availability options and costs annually with a view to seeking continuous improvements to availability, reliability, failover and throughput and to ensure Quality of Service for essential business services, and business applications solutions. This should include reviewing the department's internet bandwidth requirements and providers.

WAN Speed	NBN Fixed Wireless 50/10 Mbps	NBN 50/20 Mbps	NBN 100/40 Mbps	NBN 100/100 Mbps	NBN >100/100 Mbps	SD WAN Enabled Sites
Primary and Kindergartens	9	0	20	27	37	6
Secondary	0	0	3	1	15	1
Combined	4	0	1	4	6	1
Senior Secondary	0	0	0	0	2	0
Special/Outreach	0	0	6	0	3	0
Corporate including Libraries Tasmania	6	1	28	5	16	2
Total	**19**	**1**	**58**	**37**	**79**	**10**

Table 5 - National Broadband Network (NBN) - Summary of Connections

WAN Speed	10 Mbps	20 Mbps	50 Mbps	100 Mbps	>100 Mbps
Primary and Kindergartens	1	0	1	27	6
Secondary	0	0	0	5	9
Combined	0	0	1	13	1
Senior Secondary	0	0	0	1	6
Special/Outreach	1	1	0	3	0
Corporate including Libraries Tasmania	0	5	1	11	11
Total	**2**	**6**	**3**	**68**	**33**

Table 6 - Other WAN services – Summary of Connections

3.2 Remote Access

Remote access is the ability to gain access to the department's IT services and business application solutions from either outside the department or from a location within the department that is not considered an individual's "base location". This includes staff at non-department locations, telecommuters / mobile users (e.g. between sites) and those who are travelling interstate and overseas who may require access to the department's IT services and business application solutions. In addition to this, client groups such as teachers and students requiring access to learning management systems from their home to access classroom resources. Remote access for department staff devices is currently provided by an "always on" Cisco AnyConnect VPN Client installed to the device.

All department IT services including business application solutions will be geo-blocked so that by default they can only be accessed from within Australia and business and service delivery units will need to justify where they should be available in other broader locations.

Staff will be able to request overseas access to services like email on a case-by-case basis when they undertake work related travel.

Strategic Direction

Technologies such as Microsoft 365 and cloud hosted learning management systems enable access from a greater range of locations, thus the need for a traditional remote access solution is diminishing. The emergence of cloud remote access technologies such as Azure Virtual Desktop and Application Proxy enable access to internal department resources for staff and students. Cloud based authorisation and authentication technologies, i.e. conditional access, geo-blocking and multi factor authentication (MFA) will be essential in the provision of secure access to department IT services and business application solutions.

As part of the WoTG Networking Tasmania Core Agreement contract renewal with a focus on Secure Access Service Edge (SASE) the department should seek to adopt a Zero Trust Network Access model to improve our cyber security posture and provision of IT services to users.

Replacement Cycle

Continue to advocate for the department's remote access requirements for inclusion in the whole of government (WoTG) Networking Tasmania contracts.

As business application solutions are upgraded or modernised, remote access and authentication will be reviewed in line with contemporary policies and practices.

4 Infrastructure

4.1 Cloud Platforms

Cloud platforms provide a convenient mechanism to out-source parts of the infrastructure and application stack which reduces onboarding and development cost for new technology solutions. Broadly these service levels are Software-as-a-Service (SaaS; the entire application environment is out sourced), Platform-as-a-Service (PaaS; the computing and data environment is outsourced,

but the application needs to be developed) and Infrastructure as a Service (IaaS; only the physical infrastructure and networking is outsourced).

Tasmanian Government have had a cloud-first policy for new technology since 2017 which the department have been following since it was released. Our current preferred cloud platform is Microsoft Azure, as it offers synergy with existing technology services that we depend on (identity and Microsoft 365 office software), and offers a range of services that provide a clean migration path for legacy on-premise business application solutions hosted in Tasmanian datacentres. Currently around 70% of department application workloads are hosted on cloud platforms (IaaS, PaaS or SaaS).

As outlined in the servers/compute and application sections, the current strategy for individual workloads is to invest in solutions as high up the stack as possible (e.g. preference SaaS over PaaS, and PaaS over IaaS) as they are typically more cost-effective compared to IaaS. The service level selected will depend on the flexibility of the technology and the consumers of the system - our preference is to follow an 'adopt over adapt mantra whereby (whenever possible) business processes are changed to suite business application solutions available on the market, instead of developing software to match current business practices which are very bespoke and may no longer be contemporary. The assumption is our department is not unique and that we should be able to capitalise on investments in other sectors to reduce our system development cost, leverage business application solutions that are already developed and in use in other government departments or businesses and reduce technical debt that ultimately complicates application lifecycle management and increases the departments cyber risk profile.

Whilst cloud offers significant development benefits, it does increase operational costs as services are charged on a subscription basis rather once-off capital expense. As such there is a need to drive some cost efficiency in our cloud platforms to prevent run-away consumption increases as we move more services to cloud. Achieving this will require a combination of generating competitive pressure on cloud providers (through competitive procurement processes and contract negotiation) and adoption of shared, single-instance cloud platforms (e.g. Data Lake) whenever suited to drive service efficiency. At a technology level, our new development standards also require bespoke development to be completed in a provider-agnostic way (leveraging containerisation) which will provide an exit strategy for the department should Microsoft Azure not remain cost effective into the future.

At a staff level, we are aware that across the department there is often a view that cloud is "insecure". Industry studies have highlighted that a properly managed public cloud platform is often more secure than traditional on-premise IT hosting due to higher level of regulatory compliance reached by providers like Microsoft, and their orders-of-magnitude higher investment in cyber security funding when compared to Tasmanian Government. They also manage their services 24x7 compared to a traditional work day that most government departments use. The risk areas are around incorrectly configured platforms, and SaaS vendors that do not have the organisational maturity to adequately secure their cloud infrastructure. To manage these risks, we have developed several cyber risk assessment processes that are being applied rigorously to new product selection, and we are routinely undertaking risk and operational readiness assessments with independent parties to ensure our cloud platforms remain secure and aligned to best practice.

4.2 Servers – physical and logical

Central servers are largely virtual hosts. These servers are clustered with many virtual servers deployed to each cluster. This maximises the efficiency of server computing hardware and reduces the number of physical servers required. Current trends are to move workloads further up the technology stack to cloud-based Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), reducing the need for on-premises physical servers which are mostly housed in the Tasmanian Government data centres.

The department's physical infrastructure supporting the virtual hosting environment has passed seven years in age and is rapidly approaching end of life. The expectation is this hardware will need to be retired in the coming twelve months. Whilst significant progress has been made in moving virtual machines to cloud-based Infrastructure-as-a-Service (IaaS), the current strategy of modernising underlying platforms and opportunistically moving to Platform-as-a-Service and Software-as-a-Service requires significant planning and time and resource investment from business application solution owners. Additionally, a bulk lift and shift has been largely unsuccessful to date due to complexity. As such, ITS has adopted a combination of various approaches in moving off the ageing physical server infrastructure. These include deep analysis activities to identify servers that can be decommissioned, lift and shift of some workload and modernisation of other workload. Hardware support has been extended together with provision of extended security updates. The expectation is that the Department will have minimal business application solutions hosted in government-managed datacentres by end-2024.

For Infrastructure-as-a-Service workloads the department leverages two cloud providers. Tasmanian based Field Services Group (FSG) IaaS offering and Microsoft Azure Private Cloud IaaS. Azure Private Cloud IaaS has been found to be more scalable and cost-effective compared to FSG IaaS, whilst providing a range of value-add features that streamline integration with other cloud services such as Microsoft365. As such ITS are planning to consolidate FSG IaaS into Azure IaaS within the next five years after exiting government-managed datacentres.

Previously Azure IaaS has been procured through a Cloud Service Partner (CSP) arrangement with FSG. The CSP approach was adopted to meet requirements outlined in the original Tasmanian Government Cloud-First policy. This policy has since changed, and ITS believe the CSP arrangement exposes the department to additional cybersecurity risks and may inhibit a 'value-for-money' approach to Cloud Services by preventing the department from leveraging cost saving capabilities in Private cloud. As such ITS are intending to consolidate all Azure IaaS workloads onto a native Microsoft Enterprise Agreement subscription in alignment with existing PaaS services.

Schools are provided with a single Infrastructure Server (funded centrally) to host file shares, printers, authentication/authorisation at a local site level. With a move to Software-as-a-Service for many School-based IT Services (Microsoft Office365, email, file shares through OneDrive/Teams, on-line learning through Canvas) the requirement for local server infrastructure is diminishing. It is envisioned that several services currently hosted on physical servers will be decoupled as services like DHCP are transferred further upstream.

Whilst uptake of Microsoft365 at a school-level has increased in the last three to five years, there are still several challenges around staff training / general change management preventing widespread adoption. Additionally, cloud services do not have an offering for latency-sensitive file editing such as multimedia editing performed at some schools via the Adobe toolsets as part of

student learning programs, or for local site-based building management software. Given these challenges it is expected that some schools will need some form of local file storage capability for the next three to five years.

Strategic Direction

- Procure new workloads as far up the technology stack as possible: SaaS, followed by PaaS, private cloud IaaS, then Whole of Government IaaS, as per Tasmanian Government Cloud Policy.
- Consider opportunities to modernise existing business application solutions and take advantage of IaaS, PaaS, autoscale and geo-redundancy capabilities in private cloud.
- Continue to develop and formalise cloud infrastructure standards and reference architectures in conjunction with service providers and to provide clear guidance to software vendors on the use of cloud-based infrastructure.
- Utilise contemporary practices including Continuous Integration (CI) and Continuous Deployment (CD) to bring automation and robust processes to system deployment and maintenance. Continue to standardise on Terraform for automation given ease-of-use and support for other public clouds outside of Microsoft Azure.
- Where possible, remove dedicated Pre-Production and Development environments in favour of temporary cloned production environments and utilisation of CI / CD processes. Using CI / CD in this manner also serves as a cost management strategy for cloud and reduces infrastructure risk profile by reducing the number of permanent running environments.
- Continue to invest in training and awareness programs for ITS staff and departmental business systems staff to build understanding of contemporary, cloud-based technologies and ensure underlying assumptions about the security, reliability and suitability of cloud platforms are addressed.
- Opportunistically look to move school IT infrastructure to cloud-based solution whenever suitable. This may occur at a service/function level (e.g. move site backups to the cloud), or at a school-level dependent upon their bandwidth connection as a high speed fibre connection is preferred e.g. move several pilot schools to cloud-based infrastructure, test assumptions about suitability/performance, and leverage the pilot schools as demonstrators for the rest of department.

Replacement Cycle

- Reduce requirement for physical and virtual on-premise servers through adoption of SaaS, PaaS, and IaaS.
- Current on-premise server replacements (in schools in particular) will be considered where no alternative is available.
- Work with End Device team on Autopilot and Intune end user device software updates strategy to determine if on-site local servers for schools are required beyond 2026. Currently software distribution for end device patching / management is cached on local school servers.

Sites	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	2029/30 Devices Replaced	2030/31 Devices Replaced	Totals
4.2 Servers	71	0	0	0	0	0	0	71

Table 7 – Physical Servers

4.3 Server Operating Systems (OS)

An operating system (OS) is the software component of a server computer system that is responsible for the management and coordination of activities and the sharing of the resources of the server. The operating system acts as a host for business application programs that are run on the server. The department currently uses a variety of operating systems on its 800 servers located at over 250 locations. A portion of these are physical local site servers at school and remote business unit locations state-wide, whilst others are virtualised. Several servers are hosted in Tasmanian government data centres and host business specific business application solutions.

As services transition to contemporary cloud-based technologies such as Platform/Software-as-a-Service the operating system will become less of a concern given the OS is only pertinent for IaaS and on-premise services.

Current business application solution deployment processes on IaaS/on-premise services are highly dependent on Operating System version which leads to lifecycle management issues when the OS reaches end-of-support from Microsoft and the business application solution is still required, ultimately increasing the cyber security risk as key business application solutions are running on unpatched platforms. Effort needs to be made to decouple application dependence on server / operating system infrastructure to minimise this risk and the operational burden on IT support staff to manage them.

Strategic Direction

- During system lifecycle processes, upgrade to Windows Server 2022 which is a long-term operating system that provide five years of mainstream support and five years of extended support.
- For new systems that are unable to move to PaaS/SaaS environments, mandate automated deployment processes (preferably through CI/CD) so that the systems can be easily deployed to new infrastructure when the OS reaches end of support.
- During future procurements of new business application solutions clarify OS supportability with vendors / providers so that the upgrade path is understood (e.g. will they support current –1 operating systems).
- Continue to invest in automation capabilities for business application solution deployment and application configuration. Automation is a key to enabling cloud practices such as automatic performance scaling to meet workload / demand, continuous integration and enable deployment, and automated system lifecycle management, all of which will reduce IT

operational overheads, lower time to resolution for support issues and improve overall cyber security posture and service efficiency.

- Work with others to improve processes and policies to better facilitate wholistic lifecycle management of business application solutions. These include, but are not limited to, PaaS offerings, Windows server operating systems, database engines, .NET versions and application versions.
- Utilise the managed service provided by Patterson Brown to support legacy Solaris and Linux systems whilst progressing the migration of some of those systems to Azure IaaS/PaaS where possible, e.g. Library systems (Symphony).

Replacement Cycle

The department still has a significant number of servers running on legacy operating systems. From a support and maintenance perspective it is important that these legacy servers are actively replaced with more contemporary versions. Legacy operating systems versions increase risks, as the ability to resolve technical issues diminishes and the risk of security issues increases as the vendors develop the newer versions of the OS but don't provide the same levels of patches and updates to older versions of the OS.

The difficulty in upgrading to a new version of the OS can however be the dependencies that exist between a business application solution, and it's supported OS.

To mitigate this risk in the interim, ITS have applied extended security updates (ESU) to the Microsoft 2012 R2 Server fleet.

4.4 Infrastructure – Storage

Storage (including backup and recovery)

In the department's business units and service delivery unit areas, ITS have consolidated server disk storage to large Storage Area Networks (SANs) hosted in the Tasmanian Government data centres. These SANs are now aging and the need for replacement is diminishing due to the uptake of technologies further up the stack (SaaS, PaaS, IaaS). As with physical datacentre servers, the expectation is this hardware will need to be retired in the next 12 months, and as mentioned previously, the department is adopting a multi-faceted approach identifying those applications, servers and systems that can be decommissioned, migrated, modernised, etc.

Schools still utilise the traditional model of site-based local servers and storage however with recent investments in improved WAN services (bandwidth and redundant links) there is an opportunity to move some services to cloud-based solutions such as Microsoft365 and Canvas over the next three to five years. Some schools will still require local storage to support latency-sensitive workloads such as multimedia editing via the Adobe toolsets as part of student learning programs where cloud-based solutions are not yet fit for purpose. To protect the data stored at local sites, each School has a NAS (Network Attached Storage).

Strategic Direction

- Reduce the requirement for central storage through adoption of SaaS, PaaS and IaaS and private cloud services.
- Continue to increase bandwidth to schools whilst improving link resiliency via secondary backup WAN services to reduce requirement for local storage solutions.
- Transition existing backup services to cloud-based technologies where appropriate – initially looking to replace onsite NAS backups and offline/off-site USB backups in schools with an Azure-based solution.

Preference cloud-based solutions in schools for user data – e.g. Microsoft OneDrive for Business and Teams/SharePoint over local storage on school servers. This will continue to be a focus of discussions and actions between Teaching and Learning, Learning Services, and IT Services over the next couple of years.

Replacement Cycle

Maintain SAN based storage centrally to support legacy workloads until applications are migrated to SaaS, PaaS, IaaS, or public cloud services.

Core storage infrastructure is replaced every five years where a cloud service offering can't be utilised. On-premise storage infrastructure is upgraded / increased as necessitated by the requirements of department Business Application Solutions.

Maintain infrastructure in schools until bandwidth enables schools to only use cloud-based solutions for storage.

Migrate school backup solutions to the cloud as part of the school server refresh.

4.5 Infrastructure – Data Platforms

Databases

A database is a collection of data that is organized so that it can easily be accessed, managed, and updated. Most database technologies used by the Department are based on Microsoft SQL, with a small footprint in Oracle (library systems) and MySQL/Postgres Platform-as-a-Service for WordPress hosting.

ITS have started to leverage contemporary cloud-based PaaS databases hosted out of Microsoft Azure private cloud for new services, but have found that these offerings don't have full feature parity with traditional full-stack SQL offerings and hence are not a direct replacement for established business application solution databases.

Outside of traditional relational database management systems (RDBMS) the department have invested in a contemporary data lake architecture hosted in Azure. The Data Lake is used as a support for business intelligence reporting and orchestrating data movements between systems (as per the department's data integration standard). The Data Lake provides several benefits compared to traditional warehousing architectures including reduced cost to onboard new datasets, a more flexible data sharing architecture (that allows sharing data externally), support for both structured, semi-structured and unstructured data and improved analytics capabilities including native support for machine learning and artificial intelligence.. The expectation is the Data

Lake will eventually replace traditional Data Warehousing for the department over the next three to five years.

The continued uptake of structured data systems and the increased number of technology solutions has highlighted several data governance challenges for the department (similar to other government entities). Data governance refers to the internal standards and policy framework that dictates how data is gathered, stored, consumed and disposed across the department. Given the volume of databases across the department (over 3,000), there is a need for a policy framework and data catalogue that aggregates domain knowledge and captures information and data risk classification for the departments databases. IT Services are supporting the Data, Systems and Insights (DSI) team in the development of the policy work and have identified Microsoft Azure Purview as a technology solution to produce an automated, consolidated data catalogue to improve visibility of the departments data assets.

Strategic Direction

- Move system integration from traditional database level integration to REST APIs to facilitate further adoption of contemporary cloud-based solutions.
- Continue to invest in the Azure Data Lake as a centralised integration and reporting abstraction layer for business application solutions and associated departmental datasets.
- Continue to utilise contemporary versions of Microsoft SQL for IaaS consolidating the number of servers where possible and migrate databases from legacy versions of Microsoft SQL to contemporary versions.
- Actively decommission or migrate the few remaining Oracle based systems in partnership with the appropriate business unit as they renew / upgrade / replace the business application solution over the next two years.
- Continue to invest in the Data Lake architecture as a replacement for traditional data warehousing and opportunistically transition systems to reading from / writing to the Data Lake instead of the warehouse where required.
- Invest in organisational Data Governance practices including an Information Classification Scheme to ensure the enterprise data environment is appropriately managed and continues to add value to the department's reporting needs.
- Continue to invest in Microsoft Azure Purview as a technology solution to automate risk classification of department datasets and provide a consolidated data catalogue for department datasets.
- Utilise contractors for high level support of database environments due to their complex nature.

Replacement Cycle

Database lifecycle management closely aligns with business application solutions or services lifecycle. New business application solutions will be deployed utilising PaaS services, in turn reducing the requirement for on premises databases services.

The difficulty in upgrading to a new version of the database can however be the dependencies that exist between a business application solution and its supported database. Sometimes this dependency may mean that there is a need to upgrade to a newer database version than originally planned otherwise the upgrade cannot proceed or install a new business application solution.

Investing in CI/CD approaches for IT Infrastructure (as outlined earlier) and using application-to-application (i.e. API) integration techniques minimises the complexity of platform upgrade activities and will allow the department to be more agile with migration/upgrade activities in future.

4.6 Infrastructure - ICT Facilities

Facility Management and Hosting Services

The department broadly has two distinct IT facility management needs. These are the requirements of the main Hobart Whole of Tasmanian Government (WoTG) data centres and the requirements of other department satellite locations (schools, youth detention, learning service offices, libraries, online access centres, business unit locations, etc).

Strategic Direction

The department utilises two WoTG Data Centres currently for hosting on-premise IT infrastructure however we will seek to reduce the requirement for hosting workload within these data centres as previously mentioned. The two data centres are located at – Site A (42-24 Moonah) and Site B (42-24 Cambridge). It is envisioned that network and IT infrastructure management workloads will continue to be hosted within these data centres for some time.

- Continue to adopt Infrastructure as a Service (IaaS) via Microsoft Azure services both on-island through FSG and via Australian Microsoft data centres to reduce the requirement for local data centre services.
- Continue to adopt technology further up the stack to reduce requirement for data centre services. As part of any revised Whole of Government cloud policy, also implement other public cloud services.
- Undertake an audit of IT Server infrastructure and storage for sites, particularly schools, to inform a migration pathway for server infrastructure requirements including adoption of a serverless architecture where possible.
- Where possible migrate local site services from on premise local site server infrastructure to the cloud as WAN bandwidth and availability allows.
- Undertake a review of backup requirements at a holistic level as it applies to site data storage and the department as a whole.
- Replace UPS (uninterruptable power supplies) which support server and storage infrastructure at those sites where infrastructure will continue to exist and a full “serverless” model cannot be adopted. Further evaluate the requirement for the provision of UPS to support school office environments in the event of power failures.

Replacement Cycle

Continue to consume Networking Tasmania III WoTG Data Centre as a Service (DCaaS) during transition to cloud based services.

Reduce footprint in both department and DCaaS sites through consolidation and migration of services up the technology stack and into the private cloud where possible.

5 Infrastructure – Telephony and related services

5.1 Telephone Services

There are around 11,000 fixed lines located throughout the department including business and service delivery units, schools, libraries, and CFCs state-wide and 3,700 mobile services, with the majority of these located in schools.

Strategic Direction

All business and service delivery units areas migrated to Whole of Tasmanian Government VoIP (Cisco) in 2016 as part of the new Whole of Tasmanian Government VoIP contract. DSS is now undertaking a project to exit from this contract and offer up new services in line with modern work practices under a new Whole of Tasmanian Government panel arrangement that the department will need to procure off.

All schools currently use Small Sites VoIP (Samsung) solution under the Whole of Tasmanian Government VoIP contract. This system has now gone end of life and now needs to be replaced and is covered in the new Whole of Tasmanian Government panel arrangement that the department will need to procure off.

As we transition away from our current fixed-line telephony solutions for both school and non-school sites, DECYP in partnership with DSS will run an RFQ process looking for a strategic partner to design a telephony solution that will meet our needs for the next decade based upon the service offerings off the new Whole of Tasmanian Government panel arrangement.

Improved management of DECYP mobile phones and departmental data accessed via mobile phones will assist in improved data security and control for these devices.

Full management of a mobile device would be targeted at DECYP owned devices supplied to our users. This allows for a remote wipe of the device in the case of it being lost or stolen. It also allows for controlling web filtering and which applications can be installed on the phone. All departmental phones purchased since 2021 have been Intune enrolled which allows the device to be fully managed.

Mobile phones that are currently owned by DECYP that are not managed, will become managed when they are next replaced or will need to go through a factory reset to defaults (as if new) to have full management enabled on these devices.

In addition to managing the telephone device, there is an increased need to manage applications on the device via Mobile Application Management (MAM). This allows the department to control the data accessed by any MAM supported application. It allows the ability to remotely wipe the data and prevents copying of DECYP data outside the department. This level of management can also be applied to users personal mobile phone devices if they access DECYP data eg their DECYP email account. Whilst it allows for control of departmental data on the device, it does not affect the users personal data or their ability to use it for the personal tasks as they want.

ITS are trialling the use of MAM in anticipation of publishing a new Mobile Device Policy and Procedure which will prescribe the controls around device purchase, management, and usage

including when using personal devices to access DEVYP systems or data.

Replacement Cycle

Part of the whole of Tasmanian Government voice services contracts (there are several covering the various types of telephony services including carriage) and replacement cycles for each service type.

Mobile telephone handsets are replaced as required but normally on a minimum four year cycle.

The Samsung VoIP solution is end of life, and schools need to plan for their Samsung VoIP system replacement in their individual school IT Infrastructure plan based upon the options available under the new Whole of Tasmanian Government panel arrangement as they become available.

5.2 Video Conferencing (VC)

The department makes use of Microsoft Teams as its video conferencing / unified communications software platform. This is provided by Microsoft via its Microsoft 365 service and the annual Microsoft agreement licences all department staff for its use. Students are also covered by Microsoft Teams through Microsoft 365 as part of the department's Microsoft licence agreement.

The type of end device VC hardware required for video conferencing will depend on the use case from single users with personal VC equipment to larger units for use in classrooms or office meeting rooms.

The department's Learning Management System (Canvas) has a video conferencing function within its default configuration that is used by some schools to interact with their students.

Strategic Direction

Continue the use of Microsoft Teams as the software toolset to allow video conferences with external to government users, for administrative and educational purposes.

Use of modern Microsoft Teams Room equipment and Microsoft Surface Hubs as the hardware in any business and service delivery units meeting rooms to enable group video conferencing and collaboration to be undertaken, including with external stakeholders.

DECYP are undertaking a review process utilising industry experts to determine our future offerings in the video conference space. Microsoft have recently made fundamental changes to the Surface Hubs which has presented DECYP with an opportunity to review our current position and evaluate options in this space.

Staff continue to use personal video conferencing hardware attached to their standard department device or via the soft client software on their department mobile telephone.

In partnership with Teaching and Learning work with schools to develop various use cases of video conferencing to maximise its use including for educational learning purposes through access to Microsoft Teams in Microsoft 365, and the video conferencing component of Canvas.

The department are undertaking a review process utilising industry experts to determine our future offerings in the video conference space. Microsoft have recently made fundamental changes to the

Surface Hubs which has presented DECYP with an opportunity to review our current position and evaluate options in this space which will inform future directions for these VC use cases in future years.

Replacement Cycle

For the software component of Microsoft Teams based video conferencing solutions, the replacement cycles are enabled through Microsoft 365 evergreen processes which provide regular updates to the Teams software.

For VC hardware, continue to replace in line with device replacement cycles for personal equipment and a minimum of 5 years for room-based equipment.

The department will need to replace all Surface Hub version 1 devices before August 2025. The operating system on these devices will go end of life at this time and these devices cannot be upgraded.

Business and service delivery units	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	Totals
5.2 Surface Hubs	67	7	1	26	26	127

Schools (funded via their SRP)	2024/25 Devices Replaced	2025/26 Devices Replaced	2026/27 Devices Replaced	2027/28 Devices Replaced	2028/29 Devices Replaced	Totals
5.2 Surface Hubs	4	2	1	1	3	11

Table 8 – SurfaceHub Video Conferencing equipment

6 Cyber Security

Cyber Security services

The Whole of Tasmanian Government Cyber Security Framework and associated policies, guidelines and play books are under development by the WoTG cyber security team of the Digital and Strategic Services (DSS) branch in DPAC. Currently there is an overarching government Cyber Security Policy supported by a subset of guidelines. Once further guidelines and playbooks are released, the department will review and tailor them to suit the specific context of the services provided by the department, at which point they will undergo a formal approval process with the department Executive Committee. This work will be undertaken during the 2024 and 2025 calendar years.

Currently there is limited cyber security services available at a WoTG level. In addition to the policies and guidelines, DSS aids with Cyber Security indecent response and external vulnerability scanning services. DSS have indicated that they are working towards increasing their Cyber

capability by running a program of works that includes incident management, baseline cyber awareness, enhanced workforce capability and extending vulnerability management, however this uplift in capability has been slow to materialise.

The department has migrated its Vulnerability Management managed service onto the DSS managed service. The department is also trialling a managed Security Operations Centre for out of hours monitoring. DSS have indicated that they are not currently considering a WoTG monitoring service, and the department expects to go to market at the conclusion of the current trial in 2025.

The department uses Microsoft Sentinel, which is a scalable, cloud-native solution that provides:

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. With Microsoft Sentinel, the department gets a single solution for attack detection, threat visibility, proactive hunting, and threat response.

IT Services reports to the department's Risk Management and Audit Committee (RiMAC) on information and cyber security areas in February, June and October. This includes a summary of IT cyber security key actions and improvements. IT Services is developing a Cyber Security uplift program to better meet, and report on adherence to the Australian Signals Directorate (ASD) Essential Eight framework and its associated maturity levels.

Following on from the cyber friendly phishing training that has previously been provided, IT services will utilise the free Fortinet cyber awareness and training materials to complement the baseline service offered by DSS. A major focus will be expanding existing cyber awareness beyond Phishing to encompass more aspects of good cyber hygiene such as device and software updating, data backup and the use of passphrases.

Business Operation Support Portfolio business units have placed an emphasis on the development of Business Continuity Plans (BCP). The methods and templates devised from this development can be utilised to assist other business units in developing BCPs in their context. ITS are also collaborating with other business units to create IT Recoverability Plans for each critical business applications identified during the business units BCP process.

The ICT Acceptable Use Policy is now provided electronically to all staff each day when logging into the department's network. A Telephone and data Acceptable Use Policy, addressing the use of mobile phones and data devices, has been developed and is currently in consultation before going to the Executive Committee for approval. There are also distinct ICT Acceptable Use Policies tailored for students based upon their year level and clients of Libraries Tasmania.

Strategic Direction

The overarching strategic direction is to adopt a modern security design philosophy in all new solution deployments, which embraces a Zero Trust strategy aimed at providing protection against current and emerging threats. This strategy is underpinned by alignment with the ASD Essential Eight framework, and more broadly the ASD Information Security Manual.

ITS Cyber Security Uplift

- Increase the department's cyber security posture through the implementation and enhancement of Privileged Access Management (PAM) and Privileged Identity Management (PIM) systems, underpinned by MyLogin as the core data set.
- Continue to improve and expand the SIEM and SOAR environment by automating responses to common events and alerts based upon prior learnings across government enhancing our ability to detect and mitigate threats in near real time.
- Implement effective, contemporary security controls that are aligned with the ASD Essential Eight framework by adopting a risk-based approach to prioritise and address vulnerabilities, threats and recommendations.
- Automate the process of creating and assigning device vulnerability remediation tasks discovered by Microsoft Defender.

Data Sharing Governance Uplift

- Review, document, assess and uplift the management and mechanisms of sharing data sharing with third parties.
- Continue the development of standards, procedures and playbooks to support the evolving cyber security governance requirements.

User Education

- Develop a Cyber Security education program focusing on best practices for individuals and the protection of data using a contemporary suite of cyber eLearning resources available to all department users.

WoTG Collaboration

- Continue to collaborate with DSS at a WoTG level to leverage WoTG initiatives with the aim to leverage economies of scale or provide greater capabilities to either the department or WoTG through shared resource use.

Replacement Cycle

Continual improvement of the security toolsets as the industry matures, with emphasis on automated detection, response and remediation of emerging vulnerabilities and threats.

7 Business Application Solutions

7.1 Business and Corporate Application Solutions

The department has a complex suite of Business Applications Solutions. There are 155 applications spread out over the eight portfolios.

- **Schools and Early Years** (2 business applications)
- **Development and Support** (50 business applications)
- **Continuous Improvement and Evaluation** (30)
- **Keeping Children Safe** and **Youth Justice** (5 business applications)

- **Business Operations and Support** (64 business applications)
- **Office of Secretary** (2 business applications)

A high proportion of these business application solutions are older than 4 years. Business applications ideally should not be older than 5-7 years, otherwise there is a risk that technology and business requirements have changed too much, and support costs for the business application solutions increase dramatically. The goal should be to retire / re-engineer 15% of the business application solutions per year, which is approximately 23 applications per year. At times the cadence is increased, should operating system or technology stack components approach end-of-life and require replacement.

The department has legacy technology or process delivery still in use that no longer is considered enterprise grade, like Microsoft Access, file sharing via email inboxes, and monolithic spreadsheets in shared drives. These practices are becoming support intensive, create security risks, and are often failing to meet business requirements due to their age, size and the technology used.

Historically the department has developed business application solutions in a disconnected, reactive way. This approach has led to several problems including:

- Lack of project management discipline leading to poorly understood requirements and therefore business application solutions which are poorly aligned to business outcomes.
- Duplication of effort / data across multiple business applications.
- Difficulty in providing whole of department data analysis.
- Inconsistency of data that is stored in multiple business applications eg DECYP site locations in various business applications.
- Poor lifecycle management of the business application solutions including not undertaking regular updates (patches by the software vendors) has led to aging infrastructure (software and hardware), increasing the risk of failure of those business application solutions as well as increasing the risk to data and cyber security.
- Increased support costs for business units and ITS in supporting the multiple business application solutions and technology stacks associated with them.

Strategic Direction

- The department is developing a Roadmap for Business Applications out to 2030. An output from the Roadmap will be a Plan that covers the Business Applications.
- The preference will be for managed Software as a Service (SaaS) applications, rather than the department hosting applications and platforms. Utilising SaaS in line with Whole of Tasmanian Government Cloud strategy.
- Where this is not possible, the department will wherever possible procure off the cloud-based Infrastructure stack (Infrastructure as a Service (IaaS) or Platform as a Service (PaaS).
- The department will preference commercial solutions using industry-standard toolsets and languages with an ‘Adopt and Adapt’ approach rather than build a business application solution as a bespoke solution. Adopt means to adopt the commercial application with minimal changes and adapt our processes to fit in with the selected solution.
- ITS via account meetings with business units will be highlighting on an individual business application solution basis the underlying IT Infrastructure status of the business application,

including those at a higher risk of failure due to the server technology that hosts the application or the underlying software being aged or out of supported.

- Any new business system , significant change to a business system or new data integration must be submitted using the Technology Initiative Request which requires Portfolio Deputy Secretary approval to provide guidance to business and service areas and streamline analysis and procurement, in line with the strategic direction.
- The department utilises the Whole of Tasmanian Government Technology Services Multi-Use List (TSL) panel which includes vendors for a software development and support / services panel of local and interstate companies to enable access to multiple software solutions / technical skill sets to support business application solutions.

Replacement Cycle

This will be developed as part of the Roadmap plan.

7.2 Key Business Application Solutions Managed by IT Services

ITS provide and support a few of the department's base Business Application Solutions.

7.2.1 Content Manager

Content Manager (CM) is currently the main storage system of corporate records across DECYP and is used by all non-school staff for the storage of digital records created by Word, Excel, PowerPoint, eMail. Retention and Disposal schedules and processes are actioned on the CM storage locations on a regular basis to meet Archives Tasmania requirements.

7.2.2 ServiceNow

ServiceNow is the department's core service desk that is used by a number of business units (ITS, PSS, Finance, DSI, Libraries Tas) to manage service requests and incidents from their end users / clients streamlining their support operations, improving productivity, and enhancing customer satisfaction. It enables end users to access self help and knowledge base articles to assist in overcoming minor technical issues.

7.2.3 Identity Management (MyLogin – SailPoint)

The department's Identity Management system (MyLogin) is a contemporary SailPoint based system that uses data from key systems such as Human Resources (Empower) and Student Management System (EduPoint) to enable fine grained automated user provisioning, access, and authorisations based upon the staff or student data in the authoritive business systems. These automated processes overcome manual processes normally in place and provide a far more secure and auditable access for staff and students to business systems and associated data. This platform is constantly receiving feature and quality of life enhancements to support the access and provisioning requirements of the department, as new systems and policies are implemented.

7.2.4 DevOps

Automation of delivery – modern IT business practices like DevOps, and Continuous Integration and Deployment (CI/CD), and automated testing will be leveraged to minimise change risks, lower business application solution downtime, speed up the provision of new services, and create a flexible means to redeploy business application solutions during technology uplift programmes. Automation practices will also provide new ways of ensuring a high continuation of service and a smoother disaster recovery response should issues arise.

8 Artificial Intelligence (AI) Technology

Artificial Intelligence (AI) has generated a substantial amount of media attention over the last twelve months with the release of readily available large language models (LLM) like ChatGPT that can interpret and generate text to a level that closely simulates human conversation.

Whilst AI presents several opportunities for improving technology platforms, it is important to be aware of the risks and limitations of these products. In particular, their predisposition to hallucinate (make up answers to questions) and strong likelihood of introducing unconscious bias that may lead to misrepresentation of or negative outcomes for minority groups that were not adequately represented in the training datasets used by the LLM.

Additionally, commercially available services like ChatGPT are considered high-risk as it's not clear how data entered as prompts into these platforms is consumed and used, nor where it is stored which may ultimately contribute to a cyber breach for the department. IT Services have gained access to Microsoft AI solutions which are hosted securely in the department's cloud network environment and alleviate these risks.

Across Australia, government institutions have been rolling out ChatGPT-like solutions (e.g. South Australia's Education Chat, NswEduChat, QChat in Queensland) that are built in a secure network environment and introduce moderation layers to restrict the data returned from the AI as a way to reduce risk and provide a safe AI experience for the users. Many of these solutions are expected to be either released as open-source and/or made available to other government entities. While the AI toolset might be free, its use within a secure and safe environment controlled by the department will generate usage costs based upon the number and types of prompts used. The South Australia pilot carried out in 2023 costed this usage at $1 per student / staff member per week of use, being several thousands of $s over the school year.

At a policy level there has been significant work in this space with development of several frameworks to guide the use of AI – including the Australian government Department of Industry, Science and Resource AI ethics framework, Australian Government Department of Education Generative Policy and DECYP's own AI policy (centred on schools). Whilst students in classrooms are at higher risk of misinterpreting AI responses, there is an equal requirement to provide guidance to staff in corporate settings around the use of AI.

IT services are currently exploring several AI pilots with different DECYP business areas and industry partners, and expect the outcome of these engagements will guide the technology direction moving forward.

Strategic Direction

- Continue to align to existing federal and state AI policies as they are released or updated
- Observe roll-out of AI solutions by interstate jurisdictions, and use their learnings/technology (where available) to guide technology development.
- Preference multi-use toolsets like Azure OpenAI instead of single-use solutions to reduce cost/risk.
- Leverage pilots within the department to determine local use-cases for AI, and the overarching technology platform strategy.
- Invest in Microsoft AI technology (Copilot and Azure OpenAI) secured within the department's cloud network to manage data and safety risks.
- Ensure any technology component is supported by end user training and advice to ensure users are aware of the risks/limitations associated with their use of AI.

9 Projections of ITS Funding Allocations 2024 – 2029

IT Infrastructure – Capital - BCN 855 Business and service delivery units	2024/25 $	2025/26 $	2026/27 $	2027/28 $	2028/29 $	Total $
1.1 SurfacePro / Laptop devices (Non-school based staff)	134,200	171,600	103,400	1,467,400	3,174,600	5,051,200
1.1 SurfacePro / Laptop devices (Libraries Tas staff)	301,400	15,400	24,200	33,000	66,000	440,000
1.1 Desktop PCs, Portable devices (Libraries Tas public machines)	364,000	74,000	10,000	42,000	62,000	552,000
2.1 Local Area Network (LAN) Switches	182,931	91,267	298,487	537,249	216,368	1,326,302
2.2 Local Area Network (LAN) WAP Installation	17,000	38,143	38,143	38,143	38,143	169,572
2.3 Local Area Network (LAN) WAPs	71,000	100,468	100,468	100,468	100,468	472,872
4.4 Servers	100,000	100,000	0	0	0	0
4.5 Storage (including backup and recovery)	0	100,000	200,000	200,000	200,000	700,000
5.1 Telephone Services	20,000	20,000	20,000	20,000	20,000	100,000
5.2 Video Conferencing - Surface Hubs	871,000	91,000	13,000	338,000	338,000	1,651,000
Total	**2,061,531**	**801,878**	**807,698**	**2,776,260**	**4,215,579**	**10,662,946**

IT Infrastructure – Recurrent - BCN 855 Business and service delivery units	2024/25 $	2025/26 $	2026/27 $	2027/28 $	2028/29 $	Total $
1.1 Desktop PCs and Portable devices	8,000	8,000	8,000	8,000	8,000	40,000
1.2 Software - SOE software	914,953	914,953	914,953	1,010,000	1,010,000	4,764,859
1.3 Printers and Multi-Function Devices	0	0	0	37,500	0	37,500
1.4 IT Support Costs	110,000	115,000	120,000	125,000	130,000	600,000
2.1 Local Area Network (LAN) Switches	10,465	15,765	34,600	66,245	79,310	206,385
2.2 Local Area Network (LAN) Cabling	30,000	30,000	30,000	30,000	30,000	150,000
2.3 Local Area Network (LAN) WAPs	62,000	63,000	64,500	66,000	68,000	323,500
2.4 Network Monitoring and Management	90,000	145,000	150,000	155,000	160,000	700,000
3.1 Wide Area Network (WAN)	1,800,000	1,850,000	1,900,000	2,000,000	2,100,000	9,650,000
3.2 Remote Access	10,000	11,000	12,000	13,000	14,000	60,000
4.1 Cloud Compute (IaaS or PaaS)	3,300,000	3,400,000	3,500,000	3,600,000	3,700,000	17,500,000
4.2 Servers - physical and logical	250,000	260,000	270,000	280,000	290,000	1,350,000
4.3 Server Operating System (OS)	0	0	0	0	0	0
4.4. Backup and Recovery	209,000	209,000	209,000	209,000	209,000	1,045,000
4.5. Data Platforms	340,000	350,000	360,000	370,000	380,000	1,800,000
4.6. Facility Management and Hosting	200,000	200,000	200,000	200,000	200,000	1,000,000
5.1 Telephone Services	250,000	260,000	270,000	280,000	290,000	1,350,000
6. Cyber Security	450,000	450,000	450,000	450,000	450,000	2,250,000
7. Business and Corporate Applications Support	850,000	890,000	930,000	970,000	1,010,000	4,650,000
7.2.1 Content Manager	280,000	300,000	320,000	340,000	360,000	1,600,000
7.2.2 ServiceNow	450,000	450,000	450,000	480,000	480,000	2,310,000
7.2.3 MyLogin	600,000	620,000	640,000	660,000	680,000	3,200,000
Total:	**10,214,418**	**10,541,718**	**10,833,053**	**11,349,745**	**11,648,310**	**54,587,244**

Total - Capital + Recurrent	**12,275,949**	**11,343,596**	**11,640,751**	**14,126,005**	**15,863,889**	**65,250,190**

IT Infrastructure – Capital - BCN 823 Schools	2024/25 $	2025/26 $	2026/27 $	2027/28 $	2028/29 $	Total $
1.1 Device refresh Teacher's award	60,000	60,000	60,000	60,000	12,000,000	12,240,000
1.1 Device refresh Support staff	2,370,000	450,000	900,000	100,000	100,000	3,920,000
1.1 Device refresh Admin staff	50,000	50,000	1,496,000	50,000	50,000	1,696,000
1.1 Device refresh Yr 11 12 Extension	0	1,040,000	0	0	0	1,040,000
1.1 Device refresh Digital Inclusion Loans	0	0	1,235,000	0	0	1,235,000
2.1 Local Area Network (LAN) Switches	2,093,000	2,095,000	1,882,000	1,611,000	1,897,000	9,578,000
2.2 Local Area Network (LAN) WAP Installation	410,000	410,000	347,000	310,400	347,000	1,824,400
2.3 Local Area Network (LAN) WAPs	1,768,000	1,390,000	1,768,000	1,390,000	1,768,000	8,084,000
4.2 Servers (in Schools)	700000	0	0	0	0	700,000
4.6. Facility Management and Hosting	486000	0	0	0	0	486,000
Total:	**7,937,000**	**5,495,000**	**7,688,000**	**3,521,400**	**16,162,000**	**40,803,400**

IT Infrastructure – Recurrent - BCN 823 Schools	2024/25 $	2025/26 $	2026/27 $	2027/28 $	2028/29 $	Total $
1.1 Desktop computers, laptops and tablets	36,000	36,000	36,000	36,000	36,000	180,000
1.2 Software - SOE software	450,000	450,000	450,000	500,000	500,000	2,350,000
1.2 Software - CMP software	946,000	946,000	946,000	946,000	946,000	4,730,000
1.3 Printers and Multi-Function Devices	0	0	0	37,500	0	37,500
1.4 IT Support Costs	1,500	1,500	1,500	1,500	1,500	7,500
2.1 Local Area Network (LAN) Switches	130,500	253,400	366,000	467,000	572,500	1,789,400
2.2 Local Area Network (LAN) cabling	30,000	30,000	30,000	30,000	30,000	150,000
2.3 Wifi	636,000	636,000	636,000	636,000	636,000	3,180,000
2.4 Network Monitoring and Management	160,000	1,160,000	1,160,000	1,160,000	1,160,000	4,800,000
3.1 Wide Area Network (WAN)	4,200,000	4,200,000	4,200,000	4,200,000	4,200,000	21,000,000
3.2 Remote Access	350,000	350,000	350,000	350,000	350,000	1,750,000
4.1 Cloud Platforms	0	0	0	0	0	0
4.4 Storage (including backup and recovery)	60,000	65,000	70,000	75,000	80,000	350,000
5.2 Video Conferencing - Microsoft Teams	0	0	0	0	0	0
7.2.2 ServiceNow	450,000	450,000	450,000	480,000	480,000	2,310,000
Total:	**7,414,000**	**8,541,900**	**8,659,500**	**8,883,000**	**8,956,000**	**42,454,400**