Digital applications – policy

Contents

Read this policy with the Digital Applications Guidelines.[1] The guidelines identify different categories for approved use of digital applications and address the processes and procedures to support this policy. Approval for this policy is for five years with a review scheduled for the end of 2023.

1. Policy

The Department of Education (department) is committed to the innovative adoption and use of technology to support the active engagement of students, their learning and development in a safe and secure environment. Digital applications that capture and share private or sensitive information or pose security risks must not be used without formal assessment and approval by the department, in compliance with the Northern Territory (NT) Government Cloud computing policy.[2]

Department requirements for procurement and use of digital applications include:

- using digital applications assessed and approved for use by the department
- adhering to the Conditions of use provided by the department
- engaging in the request process to assess new digital applications.

This approach aims to reduce risk, enhance safety, create savings, and support the strategic focus of streamlining the number of digital applications in use across the department.

2. Business need

Digital applications are required across the department to support staff in the delivery of quality education services. It is recognised that evolving technology can be purchased and downloaded freely from the internet and other third-party providers. Some of these digital applications may be non-compliant with NT Government legislation or department requirements or are designed to benefit from the data they collect. The department is at risk of duplicate and non-compliant digital applications being used by staff and students. This can result in reduced data quality and an increase in the potential for harmful threats to agency information.

This policy, associated guidelines and supporting resources, outlines the requirements for all staff when procuring and using digital applications and ensures compliance with NT Government and department requirements.

3. Scope

This policy applies to all department staff, School Representative Bodies, contractors or consultants and service providers responsible for procuring or using digital applications in the NT schools environment. It determines the agency's position, roles and responsibilities for the acquisition and use of digital applications for work purposes.

Non-government schools in the NT that use the NT schools network, will be impacted by digital applications prohibited in the NT schools operating environment.

[1] https://elearn.ntschools.net/policies/letter/d

[2] https://ntgcentral.nt.gov.au/services-and-support/ict-services-websites/ict-policies-standards

Out of scope of this policy:

- non-government schools in the NT that do not use the NT schools network
- assessment of the appropriateness of content on digital applications
- advice regarding standards for development of new applications – see the NT Government Mobile application standard[3]
- this policy does not apply to information classified as 'public' as defined in the NT public sector organisations records and information management standard.[4]

4. Roles and responsibilities

4.1. Chief Executive

The Chief Executive is responsible for:

- approving the use of high-risk digital applications in the NT schools environment in line with any Conditions of use – as per the Privacy Impact Assessment (PIA) and Security Risk Assessment determined risk rating.

4.2. Information Management Committee

The Information Management Committee is responsible for:

- reviewing and endorsing the use of high-risk digital applications in the NT schools environment prior to seeking approval from the Chief Executive.

4.3. Department of Corporate and Digital Development

Department of Corporate and Digital Development is responsible for:

- completing security risk assessments for digital applications including advice on suitability and risk
- enabling integration and interface components, and other information and communications infrastructure requirements for department approved digital applications, infrastructure, and services
- providing advice for staff on information management responsibilities when using or decommissioning digital applications
- technical support and training for identified core applications.

4.4. Strategic Policy, Projects and Performance – Strategic Projects Branch

The Strategic Projects Branch is responsible for:

- approving usage of low and medium-risk digital applications

[3] https://ntgcentral.nt.gov.au/services-and-support/ict-services-websites/ict-policies-standards
[4] https://dcdd.nt.gov.au/government-records/ntps-organisations-records-information-management-standards

- providing direction on interim use of digital applications whilst awaiting an assessment
- maintaining the Digital Applications Catalogue to ensure accuracy
- managing and monitoring compliance to agreements by vendors, for those digital applications that are in the 'Integrated User choice' category
- supporting and guiding staff with requesting use of and managing digital applications
- maintaining connections with DCDD to ensure alignment of work and to optimise resources

4.5. Quality Standards and Regulation

The Quality Standards and Regulation division is responsible for:

- completing PIA and Privacy Impact Statements, once a request has been received for a new assessment
- providing professional learning in relation to privacy and the safe and appropriate use of information
- assisting staff in the management of data security breaches.

4.6. Principals and managers

Principals and managers are responsible for:

- ensuring digital applications purchased or used in their workplace or school have been assessed and approved to use and the Conditions of use are being implemented
- initiating requests to assess new digital applications
- maintaining records for all digital applications used in their workplace or school
- communicating with students, staff, and families about using approved applications
- adhering to the school or business unit responsibilities as outlined in the guidelines – including funding, training, and communicating with relevant stakeholders, where applicable.

4.7. All staff

All staff are responsible for:

- using department approved digital applications
- complying with the Conditions of use for digital applications
- initiating requests to assess new digital applications before procurement and use.

5. Definitions

Term	Definition
Conditions of use	Key information provided to staff designed to minimise risks and outline the specific rules and requirements for staff when utilising certain digital applications.
Data security breach	When personal information is misused, lost, shared, disclosed to, or accessed by an unauthorised person.
Device	A computer, laptop, tablet, mobile phone or other electronic device used for work or educational purposes.
Digital application	Any application, system, tool, or online service that can be accessed via a device, which supports the management of information, business functions and workflow processes, collaboration, and communication.
Digital Applications Catalogue	A list of known and assessed digital applications by category. To be used by staff to make informed decisions about which digital application to use or invest in.
Employee	A person employed by the Department of Education, in a school or corporate setting and includes ongoing, fixed term contract and casual employees.
High risk digital applications	Digital applications that collect personal or sensitive information or provide functionality that exposes the department to high security risks.
Low risk digital applications	Digital applications that collect no, or minimal, personal information and no sensitive information, or provide functionality that exposes the department to low security risks.
Medium risk digital applications	Digital applications that collect personal or sensitive information or provide functionality that exposes the department to medium security risks.
NT schools environment	The infrastructure provided to schools and corporate, including the internet, NT schools servers at schools and corporate locations and most devices that connect with this infrastructure. This infrastructure is supported through the Education help desk.
Privacy Impact Assessment	An assessment of a digital application's compliance against the Information Privacy Principles, as defined in Schedule 2 of the Information Act 2002.[5] It recommends risk minimisation practices for staff when using digital applications.
Privacy Impact Statement	A statement that explains in simple language how the agency manages your personal information.
Security Risk Assessment	An assessment of a digital application in compliance with the NT Government Cloud computing policy and standards and that provides risk minimisation recommendations. Conditions of use are published for users to mitigate against risks when using digital applications.
Vendor	A company or person that sells or owns a product or service.

[5] https://legislation.nt.gov.au/en/Legislation/INFORMATION-ACT-2002

6. Related legislation, policy, and documents

When implementing digital applications, the responsible party must ensure compliance with all other relevant department and NT Government policies, standards, frameworks and legislation. These include but are not limited to the following.

6.1. Legislation

- *Information Act 2002*
- Information Privacy Principles
- *Privacy Act 1988* (Cth)

6.2. Policy

- Cloud computing policy – NT Government[6]
- Digital applications guidelines[7]
- Mobile applications policy and guidelines – NT Government
- Privacy Policy

6.3. Documents

- Functional records disposal schedules – records specific to education
- General records disposal schedules
- Information Statement
- Mobile application standard – NT Government[8]
- National Principals for Child Safe organisations – Principle 8
- NT Government records management standard

[6] https://ntgcentral.nt.gov.au/services-and-support/ict-services-websites/ict-policies-standards
[7] https://elearn.ntschools.net/policies/letter/d
[8] https://ntgcentral.nt.gov.au/services-and-support/ict-services-websites/ict-policies-standards

Acronyms	Full form
DCDD	Department of Corporate and Digital Development
ICT	Information Communication Technology
NT	Northern Territory
PIA	Privacy Impact Assessment
TRM	Territory Records Manager

Document title	Digital applications – policy
Contact details	Strategic Policy, Projects and Performance, Strategic Projects, digitalanddata.doe@education.nt.gov.au
Approved by	Education Executive Board
Date approved	12 October 2022
TRM number	50:D22:66752

Version	Date	Author	Changes made
1	12 October 2022	Digital Strategy and Partnerships	First version