Procedure

Non-departmental ICT service providers procedure

Version: 1.1 | **Version effective**: 23/01/2020

Audience

Department-wide

Purpose

To outline the requirements when evaluating and procuring non-departmental Information and Communication Technology (ICT) services.

Overview

The department supports the provision of non-departmental ICT service providers for the storage and processing of data including cloud and offshore computing services to drive better performance in the department's ICT service delivery to the community and within government.

The ICT service will usually be a type of managed service under which either:

1. the provider agrees under a contractual arrangement/agreement to deliver ICT services to meet all, or part of the ICT requirements of the business unit or school; or
2. the provider manages the external delivery of ICT based services to students/parents/employees on behalf of the business unit or school. Examples of ICT services include, but are not limited to:
    - online administrative and communication tools e.g. Short Message Service (SMS) products, interview scheduling, identification 'smart' cards, conference registration, consultation and survey tools
    - online electronic document printing services specialising in printing and binding of reports/year books/newsletters/student work/calendars etc.
    - online self-paced services for curriculum related purposes such as testing and recording students' achievement or similar
    - online document scanning, electronic document management and data storage services.

Responsibilities

Employees are responsible for:

- undertaking due diligence when procuring non-departmental ICT services.

Supervisors, managers, directors, principals or above must ensure:

- due diligence is undertaken when evaluating and procuring non-departmental ICT services
- data or information stored or processed overseas with an information security classification of PROTECTED or below must be approved by the Director-General.

Principals are responsible for:

- informing and/or seeking parents/guardians, students, Parent & Citizens' Association (P&C), or other form of school council approval or support for non-departmental ICT services if required
- where procurement and use of services are not carried out in accordance with the departmental process (DoE employees only), accept full responsibility for the use of the service, including any associated risks, terms and conditions and legislative compliance (including responsibility for information involved in security breaches).

Director-General or nominated delegate is responsible for:

- approving any data/information stored and/or processed overseas with an information security classification of PROTECTED or below.

Process

ICT and ICT-enabled projects must complete an information security assessment to use non-departmental ICT services. It is strongly recommended any other procurement of a non-departmental ICT service also undertake the information security assessment. For further information contact the Information and Governance Management, Digital Transformation, I&T Branch by emailing InformationManagement.INFOMNGT@qed.qld.gov.au.

Schools wishing to use online websites or applications should follow the Service Centre Online Knowledge Base Article – Navigating the Website Risk Review Register (DoE employees only).

For all other circumstances, the following elements must be considered when procuring a non-departmental ICT service:

- **Information Security Classification.**
  Employees must consider and determine the information security classification of the information to be used or created when considering the procurement or use of non-departmental ICT services by using the department's Information security classification and handling guideline. Information with an information security classification of Protected or Highly Protected must not be stored or transmitted offshore.
- **Risk Assessment.**
  Employees must capture and manage records created in the decision process of the ICT service in accordance with the Information asset and recordkeeping procedure. This includes a risk assessment, details of the information security classification for the information, a list of the types of information managed by the ICT service provider as well as detail about the activity being undertaken. Schools should annually review these services to ensure risks are continually managed.

- **Privacy Considerations.**
  Manager, directors, principals or above who engage ICT service providers that handle personal information must:
  - monitor the service provision to prevent loss, unauthorised access, use, modification, disclosure or any other misuse of personal information
  - identify ICT service providers in privacy notices to customers where there is an established long-term outsourcing of a particular departmental function. When the ICT service provider changes regularly but outsourcing is ongoing, describe the nature of the services in the privacy notice rather than naming the ICT service provider
  - when an ICT service provider cannot be bound by a contract include an online privacy notice to customers in correspondence or on the website to indicate that the ICT service provider will hold a copy of the information and use it in accordance with their terms and conditions
  - accept responsibility for the personal information held in the service, which includes ensuring informed consent is gained and the personal information is removed when the service is ceased or decommissioned
  - seek consent from individuals if their personal information is to be used in accordance with Obtaining and managing student and individual consent procedure to use, record or disclose copyright material, image, recording, name or personal information.
- **Requirements and Consultation.**
  Principals should inform and/or seek approval or support (as appropriate) from parents/guardians, students, Parent & Citizens' Association (P&C), or other form of school council. This should include:
  - the purpose of the service and why it is to be used
  - whether personal information will be disclosed to the ICT service provider, or what information the provider is collecting
  - how personal information will be used, and whether it will be disclosed and/or transferred out of Australia. The department has no control when such information is transferred overseas.
  - requirements for gaining consent (as per the Services Catalogue Online Knowledge Base Article – Third Party Website Consent Form (DoE employees only))
  - whether the individual is able to unsubscribe from the service and how this is to be done
  - consideration of the business impact, establishment and ongoing costs, business continuity, technical interface with existing department services, risks, issues and mitigation strategies have been undertaken
  - it has an information security classification of SENSITIVE or below
  - it has been approved by the appropriate authority, and
  - it has been approved by the owner or custodian of the information.
- **Procurement.**
  If the ICT service is a paid service, follow the Purchasing and procurement procedure. Advice for protection or privacy clauses should be sought from Legal and Administrative Law Branch.

- **Approval.**
  Any data/information stored and/or processed overseas with an information security classification of Protected or below must be approved by the **Director-General**.

Definitions

Term	Definition
ICT service	Telecommunications services that carry voice and/or data and includes applications, hosting, storage, and cloud based services etc.

Legislation

- Queensland Government ICT-as-a-service policy

Delegations/Authorisations

- Nil

Policies and procedures in this group

- Nil

Supporting information for this procedure

- Nil

Other resources

- Information and Communication Technology (ICT)
- Queensland Government Digital1st strategy
- Information asset and recordkeeping procedure
- Information security procedure
- Purchasing and procurement procedure
- Obtaining and managing student and individual consent procedure
- Information security classification and handling guideline
- Personal information guideline
- Services Catalogue Online Knowledge Base Article – Navigating the Website Risk Review Register (DoE employees only)
- Services Catalogue Online Knowledge Base Article – Third Party Website Consent Form (DoE employees only)

Contact

For further information, please contact:

ICT Governance, Digital Transformation
Information and Technologies Branch (I&T Branch)
Email: ICTPolicy@qed.qld.gov.au

Review date

1/11/2018

Superseded versions

Previous seven years shown. Minor version updates not included.

1.0 Non-departmental ICT service providers

1.0 Information Communication and Technology (ICT)

3.0 Using non-departmental online ICT services where personal information is provided*

2.0 Appropriate departmental collecting, securing, accessing, amending, using and disclosing of personal information*

* indicates procedures replaced by the Information Communication and Technology procedure in 2014

Creative Commons licence