Northern Territory Government

DEPARTMENT OF **EDUCATION AND CHILDREN'S SERVICES**

# POLICY

## DATA ACCESS POLICY

| | | | |
|---|---|---|---|
| **Responsibility of:** | **Performance and Data Management** | **DET File:** | **2012/1369** |
| **Effective Date:** | **February 2013** | | **DOC2013/00617** |
| **Next Review Date:** | **February 2014** | **Version Number:** | **2.0** |
| **Target Audience:** | **Public** | | |

This policy must be read in conjunction with the **Data Access Protocol** document.

## 1. POLICY

The department will manage access to data and information as well as the data security and any risk associated with access to information held by the department.

The *Information Act* (NT) outlines that public sector organisations should make information, where possible, available to the public. The *Information Act* also states that a public sector organisation must take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification or disclosure. Care must be taken in providing access to information held by the department to minimise the risk of disclosing inappropriate information about individuals, communities or organisations.

Information collected and stored by the department's employees and those acting on behalf of the department, is the property of the department. It is a corporate resource that is utilised wherever possible to improve student outcomes in educational programs and enhance strategic and operational data driven decision making. Data is collected by the department on behalf of other organisations, under these circumstances there is a shared role in data management between that organisation and the department.

The department periodically undertakes data collections and extracts from the department's operational systems. This data provides:

- support to local and national decision making
- reporting against high level educational agreements such as the National Education Agreement, and National Partnerships
- ad-hoc and periodic reporting to internal and external clients.

The department must use personal information for the purpose for which it was collected and take reasonable steps to acquire consent for disclosure to third parties. Personal information is only used or disclosed for another purpose if that purpose is related to the primary purpose and the person would reasonably expect the information to be used or disclosed or the individual has consented to the use or disclosure.

The department may also use or disclose personal information for any other purpose if it is required or authorised by law or the use or disclosure is believed necessary to prevent a threat to an individual's or the public's health and safety.

Provided that individuals cannot be identified, the department may provide information at the school, community or organisation level in all cases excluding Australian Early Development Index (AEDI) and non-government school level data. Summary level information will be provided with a level of aggregation such that the identity of individuals cannot be reasonably identified.

## 2. BUSINESS NEED

Departmental staff frequently require data for a number of purposes as part of their job. It is appropriate to provide data to authorised employees of the department as required to perform their duties. Information obtained in these circumstances must be used in accordance with this policy, the Information Privacy Principles as scheduled in the *Information Act* as well as any other applicable regulations.

## 3. SCOPE

This policy covers all data that is held by the department including the information that is stored in the data warehouse, its associated datamarts, data sets and reports as well as data that sits outside the data warehouse.

## 4. DEFINITIONS

***Data custodian*** – The delegated officer that acts on behalf of the data owner.

***Data owner*** – The entity that has responsibility for a data set.

***Data warehouse*** – A central place where data is stored at unit record level.

***De-identified unit record data*** – Unit record data that has had any identifying information removed prior to being released.

***Identified unit record data*** – Unit record data that is identified by a code or number. For example, a student UPN.

***Name identified unit record data*** – Unit record data that is identified by an individual's name.

***Unit record*** – Data referring to a single event associated with an individual for example an enrolment or test result for an individual student.

## 5. ROLES AND RESPONSIBILITIES

The **data owner** is responsible for the quality, integrity and timeliness of the data, as well as making decisions about the collection, management and access to a data set.

The **data custodian** is responsible for making decisions on behalf of the data owner where it is impractical to seek permission from the data owner themselves. For example, seeking permission from all school principals to publish data about NT schools.

**Performance and Data Management** are responsible for the oversight of the management, governance and delivery of data including research and analysis to support evidence based policy and service delivery.

**Legal Services** can provide advice following a request for data for legal purposes including requests from the Police or legal representatives wanting access to a student's personal information.

## 6. RELATED POLICY, LEGISLATION AND DOCUMENTS

Data Access Protocol

*Information Act*

DECS Privacy Statement

## 7. ACKNOWLEDGEMENTS

Department of Health Data Access Protocol