

Data access – protocol

Contents

1. Policy summary.....	3
2. Purpose.....	3
3. Benefits.....	4
4. General principles.....	4
5. Privacy of individuals.....	5
6. Schools, communities and organisations data provision	5
6.1. Public information	5
6.2. Summary level information.....	5
6.3. De-identified unit record data	6
6.4. Identified unit record data	6
7. Protocol for data requests.....	7
7.1. Management of requests for access to data	7
7.2. Requests for legal purposes	7
7.3. Requests from the Department of Territory Families, Housing and Communities	7
7.4. Requests for linked data.....	7
7.5. Requests for official data	8
7.6. Data requests for research purposes	8
7.7. Data access approval process	8
7.8. Data access refusal	8
8. Business Intelligence Centre access.....	9
9. Data delivery and quality.....	9
9.1. Timeliness	9
9.2. Data quality	9
10. Definitions	10
11. Related legislation, policy, resources and documents	10
11.1. Legislation	10
11.2. Policy	10
11.3. Resources	10
11.4. Documents.....	10

1. Policy summary

The Data access protocol provides operational guidelines to support the Data access policy. The Data access protocol recognises that the *Information Act 2002* (the Act) outlines that public sector organisations should make information, where possible, available to the public. The 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.

2. Purpose

The Data access protocol covers all data that is held by the Department of Education (department) including the information that is stored in the data warehouse, its associated data mart, data models, data sets, reports and dashboards, as well as data that currently sits outside the data warehouse.

The department periodically undertakes data collections and extracts from the departments 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 Data access protocol provides guidelines and processes, for data owners, data custodians and internal and external clients, to manage access to and use of data and information held by the department. The Data access protocol also manages data security and any risk associated with access to information held by the department while maximising the potential for improved student outcomes in educational programs and enhancing strategic and operational data driven decision making.

The Data access protocol exists alongside the Data access policy and other agreements which relate to more specific data and data sources, for example National Schools Statistical Collection and Early Childhood Education and Care.

The Data access protocol:

- provides a streamlined and consistent process for the delivery and use of requested data including:
 - published information
 - summary level data
 - unit record data
 - legal purposes including requests from, for example, the Department of Territory Families, Housing and Communities
 - linked data
 - pre-published data
 - research purposes.
- assists in timely delivery of data.

3. Benefits

The benefits the Data access protocol provides are:

- protection of personal and sensitive information as required under the *Information Act 2002*
- reassurance for data owners of robust management of the departments data and
- an assurance that consistent and standard processes are used for provision of data held by the department.

4. General principles

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 support the departments strategic agenda and to improve student outcomes in educational programs and enhance strategic and operational data driven decision making as well as to meet obligations as an agency in the Northern Territory Public Sector. In addition to this and the Information Privacy Principles (IPP), this protocol also adopts the principles¹ that underpin the national framework for reporting on schooling. Where information is collected on behalf of another data owner, the department will become the data custodian.

- Reporting should be in the broad public interest.
- Reporting on the outcomes of schooling should use data that is valid, reliable and contextualised.
- Reporting should be sufficiently comprehensive to enable proper interpretation and understanding of the information.
- Reporting should involve balancing the community's right to know with the need to avoid the misinterpretation or misuse of the information.
- Schools require reliable, rich data on the performance of their students because they have the primary accountability for student outcomes.
- Parents and families need information about schooling, including data on the performance of their child, schools and systems, to help them to develop informed judgements, make choices and engage with their children's education and the school community.
- The community should have access to information that enables them to understand the performance of schools and the context in which they perform and to evaluate the decisions taken by governments. This ensures schools are accountable for the results they achieve with the public funding received and governments are accountable for the decisions they take. The provision of school information to the community should be done in such a way as to enhance community engagement and understanding of the educational enterprise.
- School systems and governments need sound information on school performance to support ongoing improvement for students and schools. They also need to monitor and evaluate the impacts of the use and release of this information to improve its application over time, and to assess and address the outcomes for schools and their students resulting from the public release of this data.

¹ https://acara.edu.au/docs/default-source/corporate-publications/principles-and-protocols-for-reporting-on-schooling-in-australia.pdf?sfvrsn=57674d07_0

Data is collected by the department on behalf of other organisations, under these circumstances there is a shared data management role between that organisation and the department.

5. Privacy of individuals

The *Information Act 2002* states that a public sector organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

In accordance with IPP 2 the department uses personal information for the purpose for which it was collected and takes 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.

6. Schools, communities and organisations data provision

6.1. Public information

Access to information that has been formally released and published in the public domain will be freely available. Enrolment and attendance information is regularly published on the departments Enrolment and attendance data page. The Australian Curriculum and Reporting Authority (ACARA) My School website also displays various information including enrolments, attendance, National Assessment Program Literacy and Numeracy (NAPLAN) results and more for all schools across Australia.

Provided that individuals cannot be identified, the department may provide information at the school, community or organisation level, excluding:

- Australian Early Development Index (AEDI) data – in accordance with the AEDI data protocol, disaggregated information will only be released where the data are assessed to a suitable level of confidence and validity.
- non-government school level data – may be provided internally to department staff where it is required to fulfil the duties of their position. It may also be made available to external clients where the purpose was disclosed upon collection. In all other scenarios, permission must be sought from the data owner or responsible officer to release non-government school level information. Notification of the data provision must be provided to the data owner whenever data is provided externally.

6.2. Summary level information

Summary level information will be provided with a level of aggregation such that the identity of individuals cannot be reasonably identified from the dataset alone or from a combination of other readily available datasets. All summary level reports will be assessed to ascertain whether there are any potential identification risks prior to release.

6.3. De-identified unit record data

De-identified data is unit record data that has had any identifying information removed prior to being released. This is done to avoid identification of an individual.

6.4. Identified unit record data

The department will not provide identified unit record data unless one of the following is true:

- it is the primary purpose for collecting the data
- the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the department to use or disclose the information for the secondary purpose, for example, data quality purposes
- the individual consents to the use or disclosure of the information or
- the use or disclosure is required or authorised by law.

The department may consider providing identified unit record data for research or compilation or analysis of statistics in the public interest if the following apply:

- the research, compilation or analysis will not be published in a form that identifies the individual
- it is impracticable for the organisation to seek the individuals consent before the use or disclosure
- in the case of disclosure – the organisation reasonably believes the recipient of the information will not disclose the information.

Please see the form on data requests for research purposes for more information on access to identified data for research purposes.

On provision of unit record level data, the privacy of individuals must be maintained for reporting. To ensure that confidential data is not released consideration should be given to:

- differencing – where two datasets are compared to generate a third dataset; for example, a report on enrolments in a school and a report on Indigenous enrolments for the same school, where students may not be identifiable in these two reports, but by subtracting one from the other student information may become identifiable for non-Indigenous students
- small cell size – where small numbers are present in the data it may be appropriate to suppress the cell or round numbers so that the privacy of the individuals is maintained, for example staff data for a business area that only has two staff members
- population groups – aggregates that disclose information about each individual in a group in a population may not be suitable for release, for example where a table shows that all students at a school are in a low NAPLAN band.

Data must be stored in a secure location to prevent unauthorised or accidental access, modification, loss, damage or copying.

7. Protocol for data requests

7.1. Management of requests for access to data

All requests for data must be submitted to the data custodian or responsible officer using the process described below.

1. The client contacts the data custodian or responsible officer to discuss options available, if applicable, and submits a data request to the data custodian or responsible officer. A list of contacts can be found on Data collections form and Data request form. The data custodian or responsible officer reviews the request and ensures it meets the guidelines contained within this document and the data requested is available.
2. The data custodian or responsible officer advises the client of the expected turnaround time and any issues in providing the data requested.
3. The data custodian or responsible officer provides the data to the client within the timeframes stated with any relevant caveats around the data.

Note: For requests for non-government data outside the agreed scope, additional approval will be required.

7.2. Requests for legal purposes

The department may use or disclose personal information for any purpose if it is required or authorised by law. The Quality Assurance Services unit 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.

7.3. Requests from the Department of Territory Families, Housing and Communities

An authorised officer of the Department of Territory Families, Housing and Communities (TFHC) may request identified student data under the *Care and Protection of Children Act 2007*. A TFHC request for student data form needs to be completed by the authorised officer to enable supply of this data.

7.4. Requests for linked data

The data warehouse offers a secure process by which data linkage can be facilitated to avoid disclosing identifiable unit record level data. For requests of identified data for the purpose of linking to external data sets, the guidelines set out under the identified unit record data section within this document apply. Prior to approval, consideration will be given to:

- whether the request is for summary or detailed information
- whether ethics or other approvals have been attained and
- ensuring the data is fit for purpose and that the outcome will appropriately represent the context or situation. For example, many students from urban areas may be able to be linked, but only a few from remote areas. Depending on the purpose of the request this could be acceptable if the purpose was to report on students in urban areas only but may be inappropriate if it was going to be representative of the Northern Territory.

7.5. Requests for official data

As a rule, school related data will not be provided prior to official publication. Refer to the Data collections information for details of data publication. Other data may be provided on request. School related data will be made available prior to publication to:

- principals and SAMS operators for validation of government schools data
- principals and peak bodies for Catholic and Christian schools
- principals for Independent schools
- department officers for internal purposes of planning and analysis work in accordance with the duties of their position
- meet national and local reporting requirements.

7.6. Data requests for research purposes

All applications to conduct research must first be supported by the department Research Subcommittee. If in-principle support for the research is given, the guidelines set out under the Identified unit record data in section 6.4 of this document apply.

The department may consider providing Identified unit record data for research in the public interest if the following apply:

- the research, compilation or analysis will not be published in a form that identifies the individual
- it is impracticable for the organisation to seek the individuals consent before the use or disclosure
- in the case of disclosure, the organisation reasonably believes the recipient of the information will not disclose the information.

It is at the departments discretion as to whether information is provided for research.

A Request for data for research purposes form must be completed and submitted to the appropriate data custodian prior to provision of data.

7.7. Data access approval process

The process followed by the department when determining whether data can be provided is outlined in Data request process flow chart.

These rules are subject to the data owner or data custodian being satisfied that the requesting person or organisation has a valid need for the level of data requested.

7.8. Data access refusal

If data is refused, the data custodian will provide the reason for refusal. In some cases, data may be provided at a higher level of aggregation than that requested.

8. Business Intelligence Centre access

All department staff are provided with automatic access to the Business Intelligence Centre (BIC) based on their ePass credentials, for example, principals are provided access to data for their school. When staff members change roles within the department and update their details in ePass any additional access that was granted as part of their previous role will be removed. If the additional access is still required in their new role, the staff member will need to reapply for that level of access.

The information available through the BIC is confidential and is only to be used by authorised employees of the department as required to perform their duties. Information obtained through the BIC is subject to legal and other professional privilege. This information is to be used in accordance with the Privacy Principles as scheduled in the Act, the Data access policy, protocols listed in this document, and all other applicable regulations. This information is not to be used for any other purpose, nor can it be disclosed to any third party without permission of the data owner or data custodian.

For access to BIC above the standard level, users need to complete an access request form via the Department of Corporate and Digital Development data services Jira portal. Strategic Reporting and Performance, act as a data custodian when granting access to student data. All other requests for additional access must be approved by the data owner, data custodian or responsible officer. Access to identified unit record level data held in the warehouse for non-government schools must be approved by the data owner.

9. Data delivery and quality

9.1. Timeliness

There are several factors that can affect the time it takes to provide data for ad hoc requests. Turnaround time can vary depending on the workload of the unit, the availability of the data requested and the complexity of the request. Data requested through other business units may have different turnaround times on ad hoc requests.

Department staff can readily access a comprehensive range of data through the following data sources:

- eDash, which provides schools and corporate users with access to a range of data held in the corporate systems relating to schools and students
- BIC which provides schools and corporate users with access to data held in the corporate systems relating to schools, students and staff. Standard reports in BIC are able to be developed if data is required on a regular basis
- BIC SharePoint.

Once a request has been received the data custodian or responsible officer will advise the expected turnaround time. If data is required more urgently, the request will be considered on a case by case basis.

9.2. Data quality

The department will take all steps reasonably possible to ensure quality and accuracy of data. If there are known data quality issues with the requested data, the department will endeavour to notify the client at the earliest point reasonably possible and will provide appropriate caveats on the data provided.

10. Definitions

Term	Description
Authorised officer	The Territory Families, Housing and Communities (TFHC) officer authorised under the <i>Care and Protection of Children Act 2007</i> submitting a data access request form
Data custodian	The officer who 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
Responsible officer	The officer who is acting on behalf of either a Chief Executive Officer, a data owner or a data custodian
Unit record	Data referring to a single event associated with an individual for example an enrolment or test result for an individual student

11. Related legislation, policy, resources and documents

11.1. Legislation

Care and Protection of Children Act 2007 – <https://legislation.nt.gov.au/Legislation/CARE-AND-PROTECTION-OF-CHILDREN-ACT-2007>

Information Act 2002 – <https://legislation.nt.gov.au/en/Legislation/INFORMATION-ACT-2002>

11.2. Policy

Data access policy – https://education.nt.gov.au/policies/conduct#data_access

11.3. Resources

Enrolment and attendance data page – <https://education.nt.gov.au/statistics-research-and-strategies/enrolment-and-attendance>

My School Website – <https://myschool.edu.au/>

11.4. Documents

Data access protocol document series – https://education.nt.gov.au/policies/conduct#data_access

- Data access schedules
- Data collections information
- Data request form
- Data request process flow chart

- Personal deed of confidentiality for an individual user form
- Request for data for research purposes form
- TFHC request for student data form

Acronyms	Full form
ACARA	Australian Curriculum, Reporting and Assessment Authority
AEDI	Australian Early Development Index
BIC	Business Intelligence Centre
IPP	Information Privacy Principles
NAPLAN	National Assessment Program Literacy and Numeracy
SAMS	Student Administration and Management System
TFHC	Department of Territory Families, Housing and Communities

Document title	Data access – protocol
Contact details	Strategic Policy, Projects and Performance, Strategic Reporting and Performance analysis.doe@education.nt.gov.au
Approved by	Executive Director Strategic Policy, Projects and Performance
Date approved	9 October 2023
TRM number	50:D22:79233

Version	Date	Author	Changes made
1	January 2013	Performance and Data Management	First version
2	July 2023	Strategic Policy, Projects and Performance	Review and administrative amendments to align roles and responsibilities to the structural alignment in effect from 1 July 2022, including NTG template and minor formatting, use of correct terminology, and refined to reflect practice