ACT Government Data Sharing Policy

November 2022

The ACT Government acknowledges the Ngunnawal people as the traditional custodians of the Canberra region. The ACT Government acknowledges the continuing legacy of Aboriginal and Torres Strait Islander peoples and acknowledges their vital contribution to the ACT community.

Contents

1. Introduction

Purpose

The ACT Government recognises data as a valued asset – second only to our people. We are committed to achieving our data vision of improving the wellbeing of Canberrans and visitors through the safe and effective use of data in our decisions.

The March 2020 ACT Digital Strategy signalled the ACT Government's commitment to value and responsibly use the data we collect and protect on behalf of our community. To support this, the ACT Government released the ACT Data Governance and Management Framework (DGMF) in August 2020 to build stronger, more consistent and transparent data practices.

This Data Sharing Policy (Policy) assists the ACT Public Service (ACTPS) to increase their data use for effective government operations. The sharing of ACT Government data between ACT directorates and with other approved users, such as researchers, is an important mechanism to improve outcomes for the ACT community and all Australians. The Policy demonstrates the ACT Government's commitment to privacy and security centred data governance and seeks to build trust with Canberrans on the use of the community's data.

The Policy commits the ACT Government to share data by default, where it is safe, legal, and ethical to do so, on a best-efforts basis. The Policy supports ACT Government staff to meet this obligation by providing:

- a risk-based assessment framework;
- a Memorandum of Understanding (MoU) between participating ACT Government directorates which outlines the general terms for sharing data under the Policy; and
- both an internal and external data sharing agreement template.

Scope

The Policy applies to all ACT Government data holdings where sharing is permitted under legislation and the risk-based assessment framework provided.

The Policy and its supporting materials seek to facilitate improved data sharing between ACT Government directorates. The Policy also describes the key relationships with stakeholders required to maximise the value of data across the ACT Government and community. These strategic partnerships include, but are not limited to, other Australian jurisdictions, institutions, universities, service providers, and not-for-profit and private sector organisations.

This Policy and its definition of 'data sharing' does not:

- apply to data sharing that is a legal requirement (such as information required by a court),
- apply to data sharing that is required under legislation (such as data sharing to improve reporting on national initiatives),

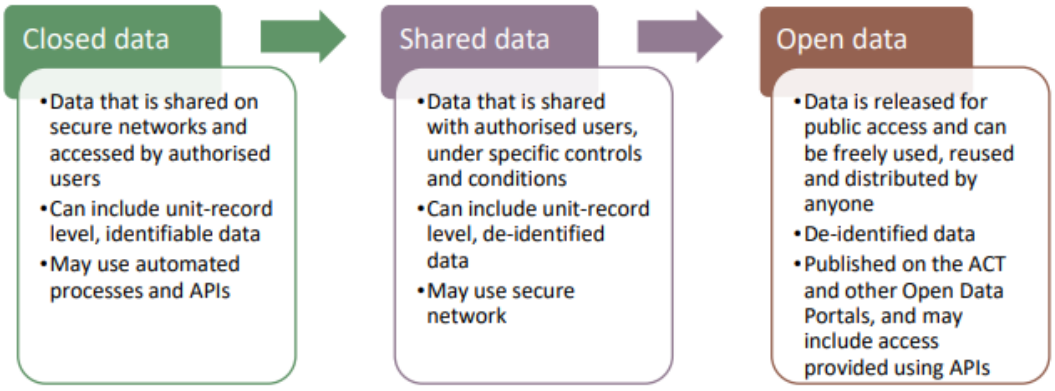
- overrule any existing or future data sharing agreements made through intergovernmental agreements or similar documents,
- address the sale of ACT Government data or any procurement processes.

What is data sharing?

The ACTPS definition for Data Sharing is:

> Making information or data 'available to another agency, organisation or person under agreed conditions.' When we share data, we are clear about who it is shared with and why, and the specific conditions, controls, and safeguards under which it is shared. [1]

This definition separates 'data sharing' from 'data release'. Data release is publishing information or data with no controls on use, also known as 'open data'. This distinction is visualised on page 78 of the ACT Data Governance and Management Guide:



This Policy uses the following definitions to key terms:

Data	Structured and un-structured information of real world observations and measurements in a raw or pre-interpreted form. Data does not contain an explicit narrative. [2]
Record	Information created and kept, or received and kept, as evidence and information by a person in accordance with a legal obligation or while conducting business; and includes information in written, electronic or any other form. [3]
Executive Data Lead (EDL)	EDLs oversee and are accountable for their ACT Government directorate's data practices. EDLs support their directorate's Data Custodians and Data Stewards to share data safely and appropriately.
Data Custodian	ACT Government staff accountable for data governance decisions for datasets and authorising safe data access, use and sharing.[4]

[1] Page 118, ACT Data Governance and Management Guide, sourced originally from the Office of the National Data Commissioner's Best Practice Guide to Applying Data Sharing Principles
[2] Proactive Release of Data Policy (ACT), Glossary, DGMF, Page 9.
[3] As defined in the dictionary of the Territory Records Act (2002), A2002-18
[4] Data Governance and Management Policy Framework (DGMF), Page 24

2. Policy Principles, Objectives, and Review

ACT Government data sharing activities are:

- community-centred and seek a community or citizen benefit,
- transparent and accountable,
- privacy and security focussed,
- ethical,
- principled and informed by established frameworks.

The objectives of the Policy are to:

- **Improve public confidence in the ACT Government's use of data** and contribute to transparent engagement with the ACT community about their data.
- **Improve and formalise strategic relationships** with Australian jurisdictions, institutions, universities, service providers, and not-for-profit and private sector organisations.
- **Reduce administrative burden when sharing data** and support ACT Data Custodians to better and more consistently request and share data safely, ethically, and legally.
- **Improved use of data and data insights in government decision making** and ACT Government policy and service design, including through research and evaluation.
- **Increased access to data** to reduce data siloing across ACT Government directorates.
- **Contribute to the improved wellbeing of Canberrans** by improving the data insights and utility of the ACT Wellbeing Framework.

The Policy should be reviewed within three years, when a significant policy or legislative change occurs that impacts the Policy, or evaluation of the policy recommends changes.

3. Data sharing in the ACT Context

Legislative framework

Data sharing in the ACT is primarily regulated by two pieces of legislation:

> The *Information Privacy Act 2014* (ACT) regulates how personal information is handled by ACT public sector agencies. The Act includes the Territory Privacy Principles (TPPs), which cover the collection, use, storage and disclosure of personal information, and an individual's access to and correction of that information.
>
> The *Health Records (Privacy and Access) Act (1997)* regulates how ACT administrative units collect, use, and disclose health information about an individual.

These are complemented by sector specific legislation. Some examples are:

> The *Children and Young People Act (2008)* sets out requirements in relation to the use of certain types of information in relation to children and young people.
>
> The *Corrections Management Act (2007)* governs the sharing of data and information in the ACT justice and corrections system.
>
> Some legislation, such as the *Working with Vulnerable People (Background Checking) Act (2011)*, specifies conditions to be met when sharing data.
>
> The *Public Sector Management Act (1994)* specifies conditions where ACT Public Service staff must disclose, or secure protected data received or created as part of their role or function.

Additionally, the following Policies and Acts have a role in governing data sharing in the ACT:

- The ACT Data Governance and Management Framework and Data Governance and Management Guide.
- The ACT Cyber Security Policy
- The ACT Protective Security Policy Framework.
- The ACT Open Data Policy.
- The ACT Information Privacy Assessment Process.
- The DDTS Cyber Security's Information Security Assessment Process.
- The Protocol for the release of data relating to the operations of the ACT Courts
- The *Territory Records Act (2002).*
- The *Freedom of Information Act 2016.*
- The *Human Rights Act 2004* (ACT)

4. Policy Mechanisms

Memorandum of Understanding

The responsibility to share

This Policy establishes a 'responsibility to share' through a Memorandum of Understanding (MoU) to drive change at an operational level. Parties to the MoU agree to use best-efforts to meet their responsibilities under the ACT Data Sharing Policy, including to:

- ensure their employees are aware of and comply with their responsibility to share data,
- encourage their employees to use the MoU and the ACT Data Sharing Policy to effectively share data and ensure the right safeguards and controls are in place, and
- ensure their staff share data in line with the ACT Data Sharing Policy, ACT Data Governance and Management Policy Framework, and any legislation or directorate specific data sharing policies guiding their data sharing activities.

The 'responsibility to share' applies when the requesting Party demonstrates that their data sharing project delivers one or more of the following public benefits:

- improved policy design,
- research and evaluation purposes,
- improved service planning and delivery,
- supports the recommendation of a Royal Commission, inquest, or inquiry,
- improved reporting activities and relevant government functions,
- supports improved public safety outcomes, and
- supports either the creation or improved delivery of a Wellbeing Indicator.

The 'responsibility to share':

- is not a legal requirement and does not override or supersede the restrictions on data sharing outlined by any current or future legislation,
- requires directorates and Data Custodians to use 'best endeavours' to share data within existing resourcing and digital infrastructure capabilities, and
- does not override a Data Custodian's assessment of a data request and their interpretation of security, privacy, resourcing, or any other considerations associated with actioning the request.

General terms for data sharing

The MoU seeks to facilitate data sharing by providing an authorising environment for ACT Government staff. The MoU also seeks to minimise the labour required by ACT Government Data Custodians to share data legally, safely, and ethically by setting out the general terms for data to be shared between ACT Government Parties under the Policy.

The MoU allows sharing agreements to specify protections and arrangements relevant to their needs through the *Internal Data Sharing Agreement Template*.

Internal Data Sharing Agreement Template

The Data Sharing Agreement Template (Template) provides a practical implementation of this policy's data sharing and management principles. The Template represents a 'standard' agreement made under the MoU, and guides ACT Data Custodian's considerations through the Five Safes and the Policy's risk-based assessment framework.

Use of this template is not compulsory to share data under the Policy. However, at a minimum, a data sharing agreement must identify: all relevant parties responsible for the data sharing activity; that it is being made in accordance with the principles of this Policy; the purpose and public benefit; and describe how the data will be safely transferred, stored, and managed in line with the ACT Cyber Security Policy.

Online Schedule of Sharing Agreements

An online, public schedule (Schedule) will provide a high-level summary of data sharing agreements made under the Policy. The Parties to the MoU agree to register a summary of any Data Sharing Agreement in the Schedule:

- what data is shared,
- the Parties involved,
- a description of the project and impacts sought,
- the outputs expected, and
- the key protections or controls used.

The Schedule seeks to promote transparent data sharing and contribute to the ACT Government's commitment to open government practices.

Additional Guidance Materials

External Data Sharing Agreement Template

The External Agreement Template is provided to support ACT Data Custodian's implementation of the Policy's principles when sharing data with 'external' organisations, such as: other Australian jurisdictions, institutions, universities, service providers, and not-for-profit and private sector organisations.

While similar to the Internal Data Sharing Agreement provided, the External Template includes additional fields and prompts ACT Data Custodian's to consider additional protections appropriate to their specific sharing arrangement.

Use of the External Agreement Template is not required to share data under the Policy. However, at a minimum, a data sharing agreement must identify: all relevant parties responsible for the data sharing activity; that it is being made in accordance with the principles of this Policy; the purpose and public benefit; and describe how the data will be safely transferred, stored, and managed in line with the ACT Cyber Security Policy.

Data Sharing Request Form

The Data Sharing Request Form (Request Form) is provided to support effective communications between a Data Requestor and Data Custodian, and ensure requests meet the minimum requirements for data sharing under the Policy. The Request Form guides Data Requestor's through the Five Safes framework and supports Data Custodian's assessment through the framework.

Use of the Request Form is not required to request data under the Policy. However, at a minimum, a data sharing request must identify: all relevant parties responsible for the data sharing activity; that it is being made in accordance with the principles of this Policy; the purpose and public benefit; and describe how the data will be safely transferred, stored, and managed to ensure data remains secure and protected from unauthorised access and use.

5. Roles and Responsibilities

Data Reform Group

This Policy empowers the ACT Government Data Reform Group (DRG) as the lead data governance group to support data sharing in the Act Government and implement this Policy. In relation to data sharing, the DRG seeks to:

- increase the use and sharing of data for evidence-based decision-making in policy, programs, service delivery and corporate management functions, and
- proactively identify and break down the barriers for staff to capture, protect, use and share data including by monitoring the progress of 'demonstration projects' and taking action on data sharing issues.

The DRG provides ACT Government Executive Data Leads (EDLs) and Data Custodians with an escalation point for advice and support. The DRG can review data sharing requests and projects, and provide advice in accordance with the principles outlined in this Policy.

The Secretariat of the DRG will:

- administer the escalation process to DRG,
- maintain the online schedule of data sharing agreements,
- coordinate the addition of any new Parties to the MoU, and
- coordinate the process of any Party's withdrawal from the MoU.

Data Custodians

Under the ACT Data Governance and Management Framework, Data Custodians are accountable for the governance of their dataset(s), including authorising its safe access, sharing and use.

Unless there is legitimate reason not to, Data Custodians must support data sharing and investigate ways to share data safely and legally. This support includes implementing measures to ensure data is captured and managed such that it can be shared safely, ethically, and legally.

Data Custodians must apply the *Five Safes Data Sharing Framework* (chapter five) when assessing sharing requests and making decisions about effective use and sharing of data.

Data Stewards

Data Stewards deliver day-to-day management of datasets and are responsible for supporting Data Custodians in their data sharing project assessments. Data Stewards must ensure all documentation relating to the data is current, and maintain accurate records of dataset's sharing, access, use, and release or destruction. Data Stewards will coordinate data sharing with the authorised users and provide technical or regulatory support.

Unless there is legitimate reason not to, Data Stewards must ensure shared data under their authority is: defined in a glossary or similar document, accompanied by appropriate metadata when shared, and well understood by the user in terms of quality and limitations.

Directorate Executive Data Lead (EDL)

EDLs are accountable for safe and competent data practices within their directorate. EDLs oversee their directorate's data management, improve data governance, and align data activities with whole of government strategic vision.

EDLs must oversee and support their directorate's Data Custodians and Data Stewards to share data safely and appropriately. EDLs are Data Custodian's first escalation point for advice, support, and remediation.

EDLs represent their directorate on the Data Reform Group.

6. Five Safes and Data Sharing Assessment Framework

The Five Safes framework (framework) is an internationally recognised risk management model used to facilitate effective data sharing by identifying and managing risk. [5] The framework enables ACT Data Custodians to assess and engage in data sharing projects by placing controls along a spectrum of five principles. Each principle ('safe') acts as an adjustable control to manage risk while maximising the utility of a data sharing project. [6] Data Custodians must apply an appropriate combination of controls to contribute to data sharing projects safely and effectively. The Five Safes are:

PROJECT	PEOPLE	SETTING	DATA	OUTPUT
How is the data being used? Who benefits?	Who is accessing the data?	Where is the data being stored and used?	What data is being sought? What protections are in place?	How are the results of the project used?

Before applying the framework, Data Custodians must first ensure:

- the data is available and suitable,
- the data can be shared legally (Data Custodians must explore how they might share data legally rather than dismissing a request due to perceived legislative restrictions),
- there are no sensitivities in the data (for example regarding commercial, legal, or privacy restrictions) that make any sharing unethical or unsafe,
- appropriate steps are taken if the sharing activity necessitates additional restrictions than are provided by a data sharing agreement (for example a deed poll or legally binding contract), and
- the costs associated with a data sharing project are commensurate with its public benefit.

Project Principle

This principle allows Data Custodians to assess the proposed benefit a data sharing project seeks to deliver. In short, this principle asks; '*is this use of data appropriate and worthwhile*?'. All subsequent principles follow from this assessment.

A Data Custodian may refer to a directorate-specific governance process to assess a sharing request. This process may include seeking advice or support from the EDL or the DRG. Data Custodians may seek additional materials from the requestor in their assessment, such as an independent ethics approval or peer review of the proposed methodology and project.

Data Custodians can assess requests through numerous criteria, but must:

- refer to this Policy's authorised purposes for data sharing established under the 'responsibility to share',
- consider existing publicly available data that may satisfy the requestor's needs, and
- if they are not the original data provider, creator, or collector, consider whether additional consultations or approvals are required.

[5] The application of the Five Safes framework in this Policy is shaped by the Prime Minister and Cabinet's 2019 Best Practice Guide to Applying Data Sharing Principles.
[6] From the Australian Bureau of Statistics' Data Confidentiality Guide on the Five Safes Framework

People Principle

This principle assesses whether the Data Requestor and/or Data User has the appropriate authority, skills, and role needed to access, analyse, interpret, and use the requested data safely. Data Custodians may assess the Data Requestor and/or User's appropriateness through their own criteria, but must at least consider the user's:

- level of capability, including their qualifications and formal accreditation,
- motivation and role, as an individual or as part of a broader organisation,
- existing authorisations from similar government bodies (such as an Australian security clearance), and
- location and the legal frameworks governing their activities, with additional assessment required for Data Requestors outside Australia.

Setting Principle

This principle assesses whether all parties have ensured data will be transferred, stored, accessed, and if required, destroyed, through processes and infrastructure that minimises the risk of re-identification or unauthorised access, use or disclosure. The Data Custodian's assessment must consider:

- whether the user will be provided real-time access to the data (such as via an Application Program Interface) or be given the data itself at a point in time (such as via download),
- the physical environment where the data will be accessed (such as an open office or controlled room or secure analysis environment),
- the IT environment in which the data will be stored and accessed (such as the network's certification, identity and access management controls, or encryption when the data is at rest), and
- whether user training is required before sharing data.

Data Principle

This principle considers what data treatments are most appropriate to manage risks of the project. Depending on the project, Data Custodians may utilise treatments such as aggregation or data minimisation before sharing with the requestor.

Each restriction applied to a dataset typically reduces its utility. Custodians should only apply treatments to data when risks cannot be managed by the other Principles of the framework. However, if Custodians can reduce the sensitivity or risk of their data without reducing the project's benefit, they must do so.

Output principle

This principle assesses what artefacts the data sharing project will create, and whether that output is appropriately safeguarded. Outputs are defined as information or data created because of data sharing, including but not limited to analyses, linking with other data, producing a publication, dashboards, reports, or other public release.

Data Custodians must be mindful of the project's outputs and their data's use in potential future projects. Data Custodian's assessments should also consider processes where project outputs may be released under the ACT *Freedom of Information Act* (2016) and ACT *Territory Records Act* (2002).

Data Custodians may consider restrictions that are:

- **rules based** – for example, that a Data Custodian must review and approve project findings before publication, and
- **principles based** – for example, that an output produced from a dataset is ethical and will strengthen the ACT Government's social license.

7. Additional resources

Further discussion and case studies of data sharing under the five safes framework can be found here:

- The Data Governance and Management Guide (page 80).
- The Office of the National Data Commissioner's Sharing Data Safely Brochure.
- In the Prime Minister and Cabinet's 2019 Best Practice Guide to Applying Data Sharing Principles.