ACT Government

Data Governance and Management Policy Framework

August 2020

ACT Government

NOTE: This ACT *Data Governance and Management Framework* was endorsed by Strategic Board on 5 August 2020

The Framework and support Guide will be designed for publishing at a later date.

ACKNOWLEDGEMENT OF COUNTRY

The Australian Capital Territory is Ngunnawal Country. The ACT Government acknowledges the Ngunnawal people as the traditional custodians of the Canberra region. The region was also an important meeting place and significant to other Aboriginal groups. The ACT Government acknowledges the historical dispossession and its continuing legacy for Aboriginal and Torres Strait Islander peoples and also acknowledges their vital ongoing contribution to the ACT community.

Contents

EXECUTIVE SUMMARY

Data is a valuable resource. Used safely and well, it has the potential to improve wellbeing in our ACT community by informing better policy, reliable programs and community-centred services. Through safe and trusted access, sharing and use of the data we hold on behalf of our community, we can continue to build community trust in government.

We use data every day and the ACT Government is committed to using data as an effective tool to deliver better outcomes for our community. However, much of our data remains under-utilised and data governance and management practices are inconsistent and fragmented across directorates.

Historically, data governance and management has been viewed as the responsibility of specific teams and individuals within government. As digital technologies change the way we work and as we seek to deliver better services through evidence-based decisions, it is imperative that our staff feel confident to safely access, share and use data.

To make the most of our data holdings, we need to know what data we have, be able to find and access it, understand when we can share it, trust in its quality, and keep it safe and secure. Inconsistent data governance and management practices pose a risk to the security and privacy of our community's data and to our ability to effectively use data to deliver outcomes.

The *Data Governance and Management Framework* (the Framework) supports directorates to build essential data governance and management practices over time, laying the foundation for a data driven culture, where data is valued for its ability to benefit our community, executives demand data to inform decisions and all staff feel comfortable and competent working with data.

The Framework provides clear, practical steps to improve data governance and management. Directorates can use the Framework to develop their data strategies and to monitor and measure their data maturity over time as we implement strong, safe practices to make the best use of our data holdings and support our community.

INTRODUCTION

The ACT Government uses data every day to deliver essential and reliable services to the ACT community. We use data to design policies and programs, and to measure their impact.

The *ACT Data Governance and Management Framework* (the Framework) is designed by and for our staff to guide how we capture, protect, use and share data. It acknowledges the importance of data in our daily work, while recognising the unique context and environment in which each directorate operates. It supports consistent, robust and principles-based data practice across ACT Government.

By investing in our data and digital capabilities, we can improve how we deliver more targeted services, achieve better outcomes for the Canberra community, while building community trust.

The Framework consists of two documents:

- The **Policy Framework** (this document) provides a high-level overview of the key elements to improve data governance and management across ACT Government and is accessible for all staff.
- The **Data Governance and Management Guide** provides a detailed, in-depth resource to improve data governance and management practice. It will support all data users, with a focus on supporting staff with a technical aspect to their role.

Framework Purpose, Audience and Use

The Framework presents 12 practical steps to improve how we govern and manage our data holdings. As we continue to move away from old ways of (siloed) working, and to orient our operations around individuals and the community, we can use this Policy Framework and Guide to build our competencies in using data to inform outcomes-focused policy and services.

The Framework applies to all directorates, staff, contractors and relevant external partners and funded service providers, and to all datasets including those located in file structures and those in managed business systems. From senior executives to staff engaged in delivering services, policies or programs, this Framework will help us all to know our responsibilities when working with and using data.

Part One – A Data Driven Culture outlines we can build a data-driven culture through establishing the following foundational governance functions: our data vision and purpose; the policy, legislation and risk environment; our data principles; roles and responsibilities; and directorate data strategies.

Part Two – A Managed Data Practice helps establish good data management processes, with the aim to improve the maturity of our data practice over time. Activities include making data discoverable; making data understood; improving data sharing; ensuring quality data; and making our data safe and secure.

Part Three - A Model to Measure Data Maturity describes how we can measure the maturity of our capabilities against the steps to better govern and manage our data.

When implemented, the 12 practical steps will enable a consistent, 'one government', continuous learning approach to how we work with data. While the framework has been designed with the public sector in mind, it can also be applied in any organisation to build our data maturity over time.

The Framework will be reviewed on a yearly basis to ensure they are continually improving, remain current and respond to Directorate needs. All data users, data custodians, data stewards and executives should reference this Framework.

12 STEPS TO BETTER GOVERN AND MANAGE OUR DATA

The Framework identifies 12 steps to guide all directorates to improve our data governance and management practice. These steps can be implemented in any order to suit their readiness and maturity.

Establish our data vision and purpose

- ☐ Develop and test directorate data vision and purpose based on the ACT data vision and purpose.

Understand the ACT policy, legislation and risk context

- ☐ Understand the relevant legislative and policy frameworks, including privacy and security provisions, and current data governance and management risks.

Know our data governance and management principles

- ☐ Embed the principles in directorate data practice.

Establish data governance

- ☐ Review and re-establish data governance groups at directorate and whole of government levels.
- ☐ Develop a directorate data governance and management implementation strategy.

Identify data roles and responsibilities

- ☐ Support all staff and executives to know their role and responsibilities in working with data.
- ☐ Ensure data custodians and data stewards actively govern and manage datasets assigned to them.
- ☐ Appoint an Executive Data Lead or ensure that the function is assigned to an existing executive role.
- ☐ Support the Executive Data Lead to uplift data practice and build a data culture in the directorate.

Build a culture that values data as an asset

- ☐ Establish and promote our shared data vision, principles and values.
- ☐ Identify barriers to achieving our data vision and embedding principles in daily practice.
- ☐ Identify and foster the desired behaviours of a data driven ACT Government.
- ☐ Measure progress towards data vision and reinforce change, and then continuously improve.

Make data discoverable

- ☐ Set up data roles, responsibilities and governance.
- ☐ Identify directorate datasets.
- ☐ Identify and train data custodians and stewards.
- ☐ Register datasets in a data catalogue.

Make data understood

- ☐ Prepare business glossary for the dataset.
- ☐ Prepare data dictionary for the dataset.
- ☐ Identify primary use of the data.
- ☐ Outline data sharing rules for the dataset.

Improve data sharing

- ☐ Foster a safe data sharing culture.
- ☐ Understand the risks, barriers and challenges to data sharing.
- ☐ Understand the legislative and policy frameworks that govern data sharing.
- ☐ Establish clear, consistent governance and management practice to enable safe data sharing, including by adopting the Five Safes principles.
- ☐ Improve open data by safely releasing more ACT Government datasets on data.act.gov.au.

Ensure quality data

- ☐ Adopt a data quality framework and standard.
- ☐ Identify and document data quality issues.
- ☐ Improve data quality and resolve issues.
- ☐ Communicate quality issues and improvements.
- ☐ Ensure staff have skills and capabilities to use data.

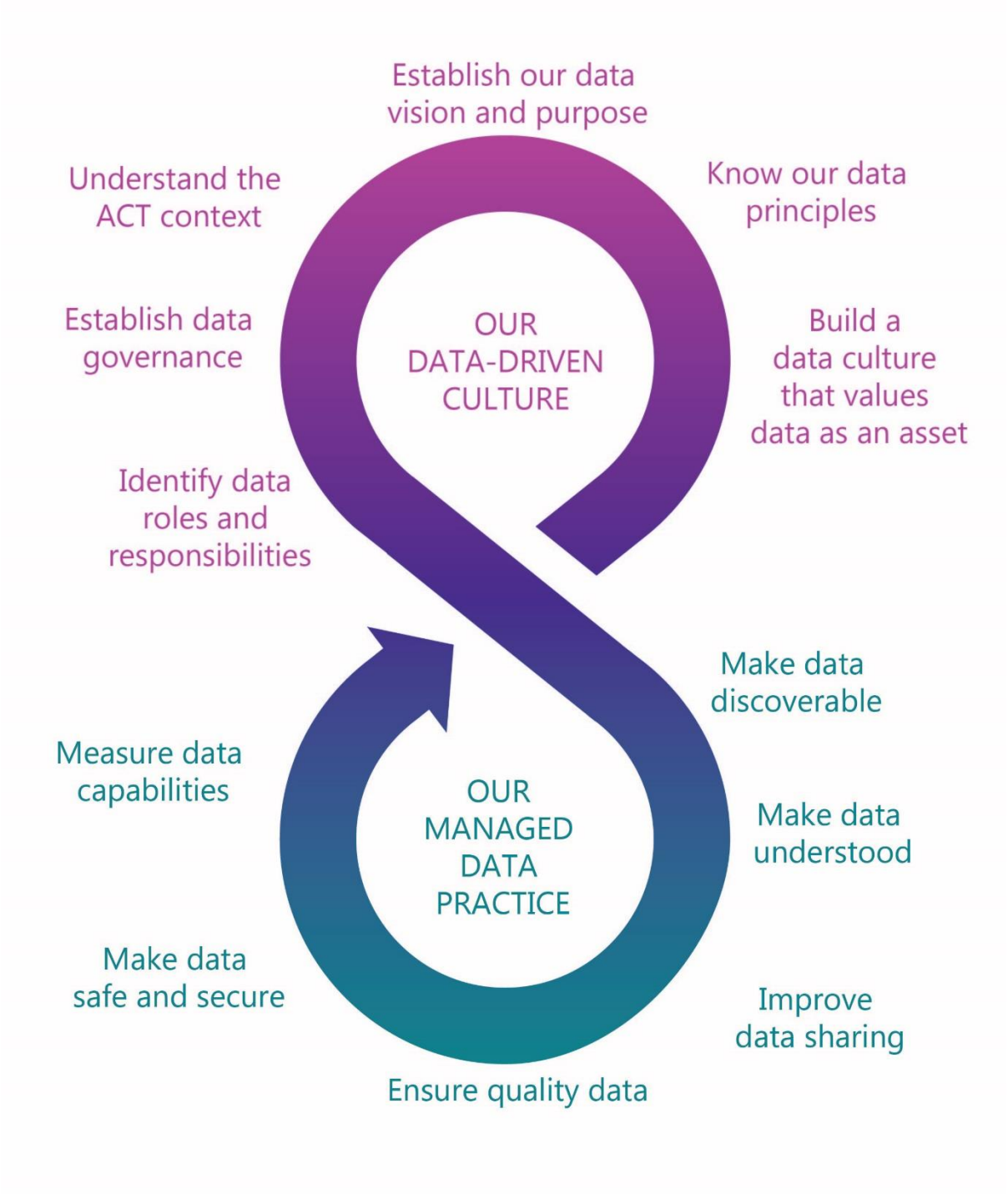
Make data safe and secure

- ☐ Establish safe data practices, technology and controls.
- ☐ Build trust in government through safe data use.
- ☐ Support staff to know their responsibilities to implement privacy and security by design.
- ☐ Establishing directorate-level data protection, including a data breach response plan.

Measure data capabilities

- ☐ Assess our data maturity against five levels: Initiate; Develop; Define; Manage; and Optimise.

This diagram of the 12 steps to better govern and manage our data represents our approach to incrementally build our data maturity through a mindset and practice of continuous learning and growth.



ABOUT DATA

What is data?

Data provides the information and evidence we need to inform decisions. We may capture original data or use data collected by other people, business areas, or organisations, where authorised. Some things are easily recognisable as data – administrative data, numbers in a spreadsheet, dates in a table. But data can also include emails, surveys, voice and video files, photographs, maps and more.

We capture data by recording real-world observations and measurements, then organise and analyse it to get information. Information and data become insights and evidence on which we can base actions when they are analysed and interpreted in the context of our work, our key lines of inquiry, and in relation to other factors and variables. We use data and digital tools, as well as critical thinking, to analyse data and to visualise and share the insights we gain with data users and decision makers.

Data can help answer questions like:

- What happened? When? Where?
- What or who was impacted?
- Why and how did it happen?
- What is needed, where and for whom?
- What works to deliver results and outcomes?
- What will it cost?
- How long will it take?
- What are the risks?

By building our data capabilities and applying consistent data principles and standards, we can:

- capture the right data on a common basis, at the right time and for the right purpose;
- combine valid and reliable data from multiple sources, across systems and regions;
- compare performance over time and/or against key benchmarks or targets; and
- communicate and report results across planning, funding, and reporting systems.

Data helps us to run the day-to-day operations and functions of government, from registering ACT road users, to hiring staff, to managing financial transactions. Quantitative and qualitative data can be used and combined with other data to improve the quality and efficiency of our operations, policies and services. They can help monitor and evaluate the success of what we do, how we do it and the difference we make. For example, quantitative analytical models can capture the measures required to identify whether an intervention has successfully delivered its outputs and achieved its outcomes, and whether it was cost effective and efficient. Qualitative methods can help validate empirical data and evidence by uncovering contextual insights such as attitudes and perceptions into what is going on and why.

Quantitative data is numerical data that can be manipulated using mathematical techniques to produce statistics. Through analysing the quantitative data, we can capture the data and information required to identify whether a service has successfully delivered its outputs and achieved its outcomes and whether it was cost effective and efficient. For example, quantitative data might include the physical locations that were burnt by the 2020 bushfires and the number of properties impacted and people evacuated.

Qualitative data is information in non-numeric form, such as notes from observational studies or focus groups, textual responses in surveys, open-ended interviews and written documents. Through qualitative analysis, we can validate empirical data and evidence by uncovering contextual insights, helping us understand attitudes, opinions, perceptions, values, concerns and motivations. For example, qualitative data might include the stories of people living in bushfire-affected areas during the 2020 fires, such as the physical, emotional and psychological impact the bushfires had on them, their families and friends, how they are recovering, and their readiness for the next bushfire season.

The data lifecycle

Data tends to follow a cycle over which we generate its value to inform our work: from initial capture based on a need or purpose to when it is no longer used for that purpose. This Framework provides a series of processes that can be applied when managing data to ensure that staff who rely on data can discover, access and use it, trusting in its accuracy and timeliness.

Further detail about each step of the data lifecycle can be found in the *Data Governance and Management Guide*.

What is data governance and management?

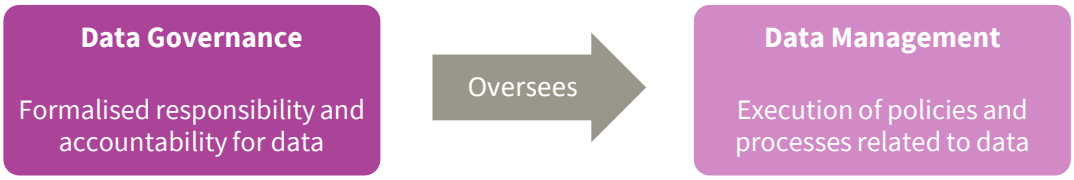


Diagram adapted from ONDC.[1]

It is important to understand the differences between data governance and data management: data governance is the policy-making framework for public sector data while data management involves execution of those data policies set by the ACT Government and the directorate.

Data Governance

Data governance involves making decisions about how data can be captured, protected, shared and used. It ensures key staff across the ACT Government are accountable for the appropriate handling of data and provides critical oversight of data management practices. It represents a structured and formal commitment by the ACT Government to taking a proactive approach to building privacy and protections into the design, operation and management of our processes and systems. It establishes decision-making and accountable bodies to oversee the development and implementation of data policies and data management practices such as standards, guidelines, business rules, decision rights and processes.

Data Management

Data governance is supported by effective data management practices and processes to ensure trusted access, sharing and use of data for community benefit. Data management is a multidisciplinary approach to organise and handle data that includes developing, implementing and overseeing processes to capture, protect, use and share data. It provides the foundation to make our data assets discoverable, trusted, accessible and secure, and provides a basis for building a data-driven culture across ACT Government that will help us to realise the full value of our data assets.

[1] Office of the National Data Commissioner (2020) *Foundational Four: guidance for agencies to improve their data practices*, available from <https://www.datacommissioner.gov.au/media-hub/foundational-four-guidance-agencies-improve-their-data-practices>

DAMA Data Governance and Management Disciplines

The Data Management Association's *Data Management Body of Knowledge* (DAMA DMBoK) identifies 11 functions or 'Data Management Knowledge Areas' that together form the foundations of good data practice. Good data governance is necessary for consistency and balance between these areas.

The Framework learns from and applies the DAMA DMBoK functions in the ACT Government context, allowing flexibility for the unique characteristics of each directorate. The Framework and Guide presents these functions into a set of pragmatic steps for directorates to the design and embed these functions in practice. The functions are described below, with definitions drawn from DAMA DMBoK.[2]

Data governance	Provides planning, oversight, and control over the management and use of data and data-related resources. Data governance is placed at the centre of data management activities, since governance is required for consistency within and balance between the functions.
Data architecture	Defines the blueprint for managing data assets by aligning with organisational strategy to establish strategic data requirements and designs to meet these requirements.
Data modelling and design	The process of discovering, analysing, representing and communicating data requirements in a precise form called the *data model*.
Data storage and operations	Includes the design, implementation and support of stored data to maximise its value. Operations provide support throughout the data lifecycle from planning for to disposal of data.
Data security	Ensures that data privacy and confidentiality are maintained, data is not breached, and data is accessed appropriately.
Data integration and interoperability	Includes processes related to the movement and consolidation of data within and between data stores, applications and organisations.
Document and content management	Includes planning, implementation and control activities used to manage the lifecycle of data and information found in a range of unstructured media, especially documents needed to support legal and regulatory compliance requirements.
Reference and master data	Includes ongoing reconciliation and maintenance of core critical shared data to enable consistent use across systems of the most accurate, timely and relevant version of truth about essential business entities.
Data warehousing and business intelligence	Includes the planning, implementation and control processes to manage decision support data and to enable knowledge workers to get value from data via analysis and reporting.
Metadata	Includes planning, implementation and control activities to enable access to high quality, integrated metadata, including definitions, models, data flows and other information critical to understanding data and the systems through which it is created, maintained and accessed.
Data quality	Includes the planning and implementation of quality management techniques to measure, assess and improve the fitness of data for use within an organisation.

[2] DAMA (2017), pp45-46

PART I
A DATA-DRIVEN CULTURE

The steps in this section helps us to build good data governance practices so that we can move to a data culture where our employees drive purpose in trusted and safe use of data.

- Establish our data vision and purpose
- Understand the ACT policy, legislation and risk context
- Know our data governance and management principles
- Establish data governance
- Identify data roles and responsibilities
- Build a culture that values data as an asset

ESTABLISH OUR DATA VISION AND PURPOSE

The ACT Government seeks to improve the wellbeing of our entire community so that we can all reach our full potential. Public services such as schools, hospitals, transport, child protection and community safety, as well as planning, infrastructure and city services can enhance outcomes and transform lives and livelihoods. This is particularly important for people with diverse and complex needs and for those experiencing any form of vulnerability, disadvantage, or marginalisation. To foster a sustainable, resilient and vibrant community, government services depend on having all the relevant information to support better planning, strong decision making and effective service provision.

We **value the data we capture, protect, share and use on behalf of our community**. We want data to be captured, managed and used in a way that protects privacy and develops better services for the community. Data is a cornerstone to a truly digital government.

OUR DATA VISION:

To enhance the wellbeing of Canberrans and visitors through safe and effective use of data in our decisions.

The purpose and importance of data governance and data management for the ACT Government

The ACT Government is growing our use of data to support a more connected Canberra, making life better for Canberrans and the businesses that employ them. We are also improving how our staff can access the broad and disparate range of data we hold, making data use safe and trusted, enhancing data capabilities and skills, fostering a learning culture and empowering staff to make data-driven decisions.

The Open Data Policy (2015), the establishment of the Office of the Chief Digital Officer (OCDO) and ACT Data Analytics Centre (ACTDAC), and the recent moves to reform the ACT Government's information and data sharing systems and processes, signal a whole of government commitment to improving safe data capture, use, sharing and release.

With the increased access and use of data come increased risks to security of personal and sensitive information, as well as legal and ethical considerations in the use and reuse of data, and the ongoing need to earn and maintain public trust and confidence in how we use and secure the community's data.

Currently, there are inconsistent and varying levels of maturity in data governance and management practices across the ACT Government. Staff report common challenges in finding and accessing data, a lack the contemporary skills and capabilities to work with data, a lack of familiarity with their roles and responsibilities related to data, and lack of confidence in sharing and reusing data.

To realise our data vision, we need a proactive approach that will build and strengthen data skills and capabilities, and to actively and diligently remove barriers for our staff to capture, protect, use and share data.

By implementing this Framework, the ACT Government will improve the maturity of our data governance and management practice and to enable and empower our staff to better realise the benefits of data to

inform public policy and services. The Framework will support directorates to establish rigorous and robust controls, governance and agreements regarding the access, use and release of data and it helps to build and maintain public trust and confidence in government use of data.

Strong, consistent data governance and management practices, will help us deliver better outcomes for our community:

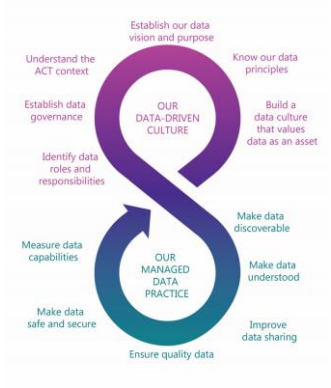
- When all staff feel confident to work with data and understand the responsibilities around data that come with their role,
- When we increasingly share and use data for evidence-based decision-making, policies and programs, resulting in better services for our community.
- When we demonstrate that our approach to working with data is respectful, secure, accountable and transparent, we build the community's confidence that government uses and shares their data appropriately, resulting in greater community trust in government.
- When we increase the release of ACT Government data on the open data platform we are transparent and accountable to the community about our data holdings and we support community engagement and health and wellbeing, unlock innovation and enable businesses to uncover new opportunities, resulting in a community that is better connected and empowered to make decisions.

ACT Government Data Vision and Purpose – Logic Map

Data governance and management practices are consistent across ACT Government directorates

The *Data Governance and Management Framework*

- articulates the data principles and common language for establishing foundational data practices and behaviours
- guides directorates to improve capabilities to safely acquire, capture, protect, use and share data
- is a living document that will evolve as we transform and mature our data and digital capabilities over time.



We value data as an asset and its potential to benefit the community

We know what data we hold and can find it

We safely and efficiently share information and data with purpose, while protecting privacy

We ensure data is fit for purpose and can be used in decision making

We protect the security and safety of data assets and build privacy into data systems and processes

We understand our roles and responsibilities and competently and safely work with data

We know, trust and use data in the decisions we make on behalf of the ACT community

We consciously learn, adapt and transform how we work using data

We earn and maintain public trust

Respectful We listen to community views and use data appropriately and ethically

Secure We proactively manage risks, protect the privacy and security of personal information

Accountable We respond quickly when things go wrong, are honest about mistakes and learn from them

Transparent We openly and proactively communicate about how we capture, protect, share and use data

Our community receives better and more targeted services, policies, planning, and research

Our community trusts that we are responsive to their needs through safe use of data

Our community trusts in government to use and protect their information

Our community is better connected and empowered to make decisions

Better wellbeing for our Canberra community

By taking advantage of advances in data and technology, the ACT Government supports our community to achieve better outcomes in health and wellbeing, safety, productivity and connectivity, supporting Canberra to be one of the world's most liveable cities

UNDERSTAND THE ACT POLICY, LEGISLATION AND RISK CONTEXT

The ACT Government provides and funds a wide range of services for and on behalf of the community. These include education, health, housing, transport and roads, environment, business investment, and city and community services. The community sector, private sector, and the Australian Government also contribute to delivering services to our community.

ACT and national level strategies, policies and legislations guide our day-to-day work. As a result, this Framework sits within a complex ecosystem that defines how we capture, protect, share and use data. A selection of relevant legislation and policy are outlined below, noting that this is not an exhaustive list and does not include all portfolio-specific legislation that may be relevant for directorates.

Australian Government and National Legislation and Policy	Privacy Act 1988 (Cth)	Public Sector Management Act 1994
	Freedom of Information Act 1982	Healthcare Identifiers Act 2010
	Data-matching Program (Assistance and Tax) Act 1990	Data Availability and Transparency Bill (forthcoming)
	Public Data Policy Statement	Public Sector Data Management Project
	National data agencies and partnerships including the Office of the National Data Commissioner and the Australian Data and Digital Council.	
ACT Legislation	Information Privacy Act 2014	Health Records (Privacy and Access) Act 1997
	Territory Privacy Principles (TPPs)	Children and Young People Act 2008
	Human Rights Act 2004	Domestic Violence Agencies Act 1986
	Territory Records Act 2002	Crimes (Sentencing) Act 2005
	Freedom of Information Act 2016	
ACT Policy	ACT Digital Strategy	
	The Privacy Data Breach Management Policy: Information Privacy Act 2014 (forthcoming)	
	ACT Government ICT Incident Response Plan	
	ACT Government Risk Management Framework and Policy 2019	
	ACT Government Protective Security Policy Framework 2017	
	ACT Government Protective Security: Information Security Guidelines 2017	
	ACT Government ICT Security Policy	
	ACT Government Sensitive Information Encryption Standards 2020	

In 2019, directorates agreed to an information and data sharing approach of 'sharing by default except where there is a good reason not to', moving away from a widespread culture of 'if in doubt, don't.' Directorates are responsible for building an awareness and capabilities for sharing data *by default*. Over time, the ACT Government may consider introducing new policy and/or legislation to enable data sharing, like other jurisdictions.

Our current data governance and management experience and risks

The following common barriers and challenges relating to data governance and management have been identified across ACT Government. These ongoing risks to data and data practice can be better managed through implementing this Framework and its supporting resources.

Data **capabilities and infrastructure are varied and inconsistent**, with a lack of proactive data practices, systems and mechanisms to enable staff to search for, find, access, share and use data.

Data **governance and management practice is inconsistent** across government, with varying levels of maturity across directorates, staff not aware of their roles and obligations, a lack of consistent and common language around data, fragmented data collections and sporadic data releases.

Staff face **challenges accessing data**, due to behavioural, cultural, technical and legislative barriers to data sharing.

Staff **don't know where to find data**, or what data exists to support their work; directorates lack a consistent way to list data holdings with no whole of government data registry or catalogue.

Staff **can't trust data due to a range of quality issues** and inconsistent data breach practices. Data custodians are not always aware of their role in ensuring and improving data quality and useability.

Data is contained in legacy information technology systems, and designed in silos, with a lack of common data definitions or standardisation between systems, with no provision of metadata and inconsistent storage formats.

Staff **don't know how to work with data** and lack data and digital literacy and skills. Staff across directorates need support to release data on the ACT Government open data portal at data.act.gov.au.

Data **security practices and processes are fragmented and inconsistent** across directorates, with a lack of understanding about data safety and security risks and who has responsibility for managing those risks. There is an absence of proactive and responsive processes and records of actions taken.

Some existing barriers and challenges have been identified that are specific to data sharing, including:

A **risk averse culture** that impedes the sharing and reuse of data due to:

- longstanding experiences and a genuine lack of understanding about when, why and with whom data can be shared;
- poor quality of the datasets and mistrust in the capabilities of data users;
- mismatch between community expectations to share data and a fear of undermining trust; and
- few direct consequences for withholding data even when there is a legal basis or community expectation to do so, and fear of repercussions for inappropriate disclosure or use.

A **complex legislative environment** within directorates and across government can make it difficult for individuals to understand whether data can or can't be shared.

Inconsistent governance, policies and data management practices within and across directorates, preventing staff from confidently making decisions to share information and data.

Outdated digital infrastructure where data is manually extracted, cleansed and shared through ineffective and unsecure mechanisms that may not support privacy-centred data distribution.

OUR DATA GOVERNANCE AND MANAGEMENT PRINCIPLES

We are community-centred	• We actively and respectfully engage with people and the community to understand and address their needs and concerns about the data we capture, protect, share and use on their behalf.
We are transparent and accountable	• We openly and proactively provide clear, accessible information to the community about how we collect, manage and use data. • When things go wrong, we respond quickly, are honest and learn from our mistakes.
We share and use data safely	• We share data to benefit the community, while proactively protecting the privacy of individuals. • We ensure appropriate and ethical use of data, in accordance with legislative and policy requirements.
We are skilled and capable	• Our staff are empowered with appropriate skills, knowledge and capabilities to work with data. • Our staff know their responsibilities and obligations to ensure safe and trusted capture, use and sharing of data.
We make data discoverable	• We know what data is available and how to find it by ensuring data is clearly and explicitly described and registered in a searchable resource.
We make data trusted and secure	• We make data quality known and manage data integrity and consistency. • We are proactive in protecting the security of the data we hold and use on behalf of the community.
We value data	• We use data to inform evidence-based policies, programs and services that improve outcomes for our community. • We treat data as an asset because we recognise the potential of data to benefit our community.
We make data open	• We make ACT Government data freely available for public access and use to support community wellbeing, innovation and growth.

This section supports ACT government and directorates to take a consistent approach to establishing data governance arrangements to oversee the way we capture, protect, share and use data to benefit our community.

We establish data governance through these steps:

1	Review and re-establish data governance groups at directorate and whole of government levels
2	Develop a directorate data governance and management implementation strategy and roadmap

Robust data governance arrangements can improve the visibility and availability of data, create the foundations for fostering a data-driven and evidence-informed ACT public service, and demonstrate that we value the data we capture, protect, share and use on behalf of the community.

There are four components to good data governance arrangements:

- Embedding our **data governance and management principles** (page 18)
- Establishing **data governance groups** to be accountable for data-related decisions (page 21)
- Developing a directorate **data governance and management implementation strategy** and roadmap (page 22)
- Identifying and assigning **data roles and responsibilities** (page 23).

Directorate data governance and management implementation strategies and roadmap

The *Data Governance and Management Guide* provides a detailed guide to developing a directorate data strategy in the *Establish Data Governance* chapter and at Appendix II.

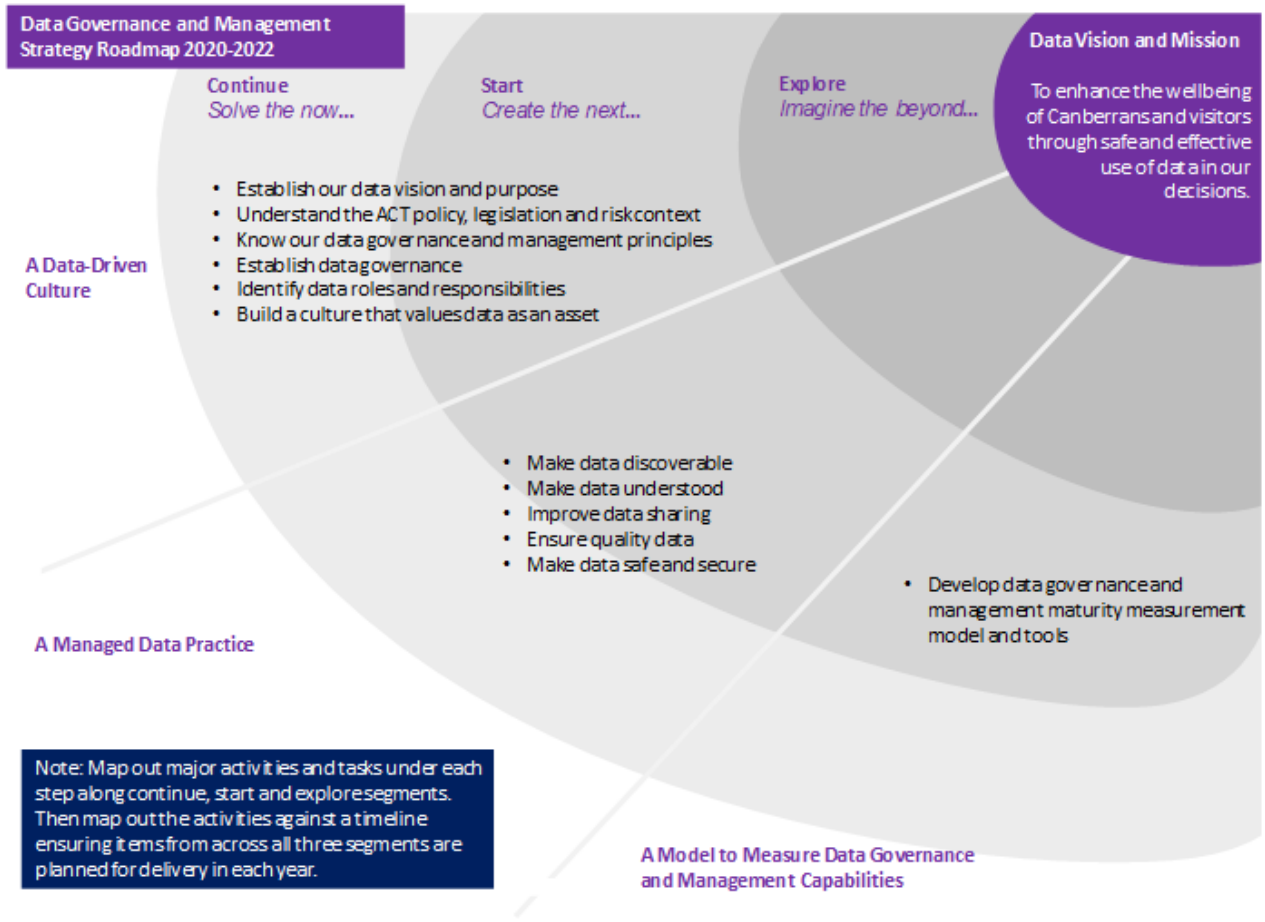
In developing a data strategy, it is important that directorates:

- establish the authorising environment in which to develop a strategy and change journey;
- consult extensively to understand existing barriers and challenges;
- identify clear focus areas including to lead a change journey;
- identify what a successful outcome will look like; and
- identify how to communicate the strategy, vision and desired change, and stories of progress.

An implementation roadmap sets out the steps to implement the directorate's data strategy. It can help to identify and communicate what a successful data strategy will look like. It should be simple, with the goal of iteratively building culture and improving data practice over time.

From the first year of the roadmap, directorates should build in activities that **continue** good data practices, to enhance and improve existing activities, **start** identifying new approaches and **explore** what may come next, uncovering opportunities to better support our community through emerging technologies.

The following sample graphic depicts the way in which we may choose to depict the 12 steps with associated activities such as to design and implement key activities, processes, tools and resources.



Whole of government data governance arrangements

Data governance arrangements for the ACT Government are founded on the notion that good governance is manifested in accountable decision-making, where staff acting across the strategic, tactical and operational layers lead the change to achieve better data practice. The desired change is outlined in the logic map in the 'establish our data vision and purpose' section of the Framework.

The ACT should develop a cascading data governance model across these three layers. It is recommended that staff understand the whole of government data governance structures when planning the directorate's approach to enhancing data governance. This is outlined in the table below.

ACT government established the Data Steering Committee and two sub-committees, the Data Management Committee and Privacy and Risk Committee in 2018. With the release of this Framework, these committees will be reviewed to ensure they evolve to provide greater value across government.

		ACT Government*		Directorate	
Strategic	• *High level oversight of data practice* • *Address systemic barriers* • *Allocates resources to strategic priorities and innovative enablers*	**Strategic Board** • Provides whole of Government leadership and strategic direction for Data Governance and Management in the ACTPS. • Fosters data culture across the ACTPS • Membership includes the Directors-General of all ACT Government directorates, and other Executives as appointed.		**Directorate Executive Board** • Provides leadership and strategic direction for the Directorate. • Membership includes the Director-General, Deputy Directors-General and other Executives as appointed.	
Tactical	• *Active oversight of data practice* • *Identify risks, issues and remove barriers through innovation* • *Plan, coordinate and apply resources including data infrastructure, and resources*	**Data Steering Committee** • Leadership to monitor, protect, prioritise and develop the ACT Government's data assets. • Allocates resources across data projects and data ecosystem	**Chief Digital Officer** • Drives data and digital transformation • Accountable for guiding consistent data practice • Point of escalation for cross directorate data issues • Oversees the work of ACTDAC	**Data Governance Committee** • Align with ACT Government strategic priorities. • Sets directorate data priorities and roadmap • Oversees directorate data management practice improvement	**Executive Data Lead** • Builds data and digital culture • Implements Data Governance and Management Framework. • Point of escalation for data risks and issues within directorate.
Operational	• *Day to day operations to achieve outcomes and maintain continuous improvement* • *Ensure consistent data governance and management within Directorate and partners* • *Manage operational risk, monitor performance and compliance, and escalate barriers*	**Data Management Committee** • Develops and guides implementation of the ACT Data Governance and Management Framework. • Contributes to whole of Government data governance and management activities eg master data management and data analytics platform.	**Data Privacy and Risk Committee** • Examines, advises and/or coordinates whole of Government approaches to address risks associated with legal, privacy and ethical considerations for data use, sharing, retention and disposal.	**Data Custodian** • Subject matter experts driving execution of the framework, strategy and roadmap in their line areas. • Other roles identified in this document also support the framework execution.	**Data Steward**
		Data Community of Practice • Data novices, specialists, practitioners, leaders and people interested in data come together to share ideas, solve problems, connect with peers, and build capabilities.			

*The ACT Government data governance arrangements will be reviewed from time to time to ensure we keep abreast of the changing data ecosystem, changes in government context and directions, as well as to meet community expectations.

This framework signals the importance of connecting data with digital functions. As such, the ICT governance groups that oversee and monitor the risks and return on ICT investment and delivery, also have a role to support implementation of this framework. These include the Digital Services Governance Committee, the Geospatial Advisory Sub-Committee and the Architecture Design Review Panel. Further detail on whole of government groups and committees is provided in the *Data Governance and Management Guide*.

Office of the Chief Digital Officer

The Office of the Chief Digital Officer (OCDO), which includes the ACT Data Analytics Centre (ACTDAC), supports directorates to implement consistent data governance and management practices and provides support to the whole of government data governance committees.

The OCDO was established in 2015 to drive the ACT's digital and data transformation agenda, lead the whole of Government strategic direction for ICT and reports directly to the Head of Service and the Chief Minister, working with Strategic Board (comprising all Directors-General) to ensure whole of Government solutions.

ACTDAC was established in 2018 to provide an ACT-wide data analytics capability and help improve the management, use and reuse of government data to create public value and benefit. ACTDAC supports directorates to improve data governance and management practices, enabling safe and trusted sharing and public release of government data assets.

Directorate data governance arrangements

Ensuring good data governance within directorates involves maintaining appropriate leadership and accountability structures that are fit for each directorate's context, core accountabilities and service environment. Directorates should:

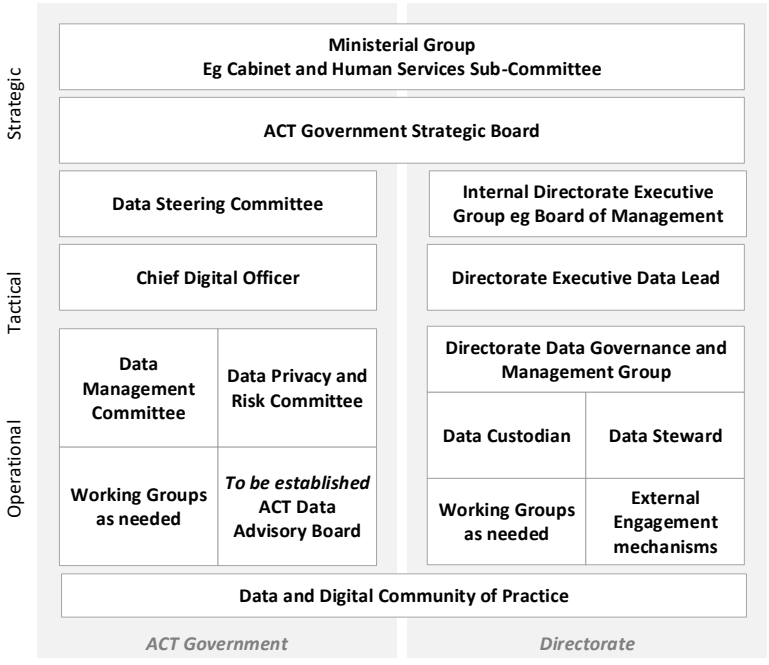
- identify and establish internal data governance bodies to oversee the implementation of this framework;
- develop policies and procedures for data use and management in accordance with the ACT data governance and management principles;
- establish directorate data governance and management implementation strategies and roadmaps;
- identify and appoint people with data-specific roles and responsibilities to support data governance, management and use; and
- foster a data culture, build staff capabilities and manage change.

While data governance should be consistent across ACT Government, each directorate will decide its implementation approach. Directorates may choose to refresh existing or establish new data governance bodies or groups.

Membership of data governance bodies will include the directorate Data Executive Lead, data custodians and data stewards, with other directorate executives and staff as needed.

Directorate data governance bodies are responsible for developing and implementing the directorate's approach to embedding the data governance and management principles, including developing a directorate data strategy and roadmap as set out in this Framework.

It is important that data governance within the directorate is supported at a senior executive level to foster a data culture within the directorate, develop buy-in from staff, build accountability for safe and trusted use and sharing of data, and ensure successful implementation of the directorate data strategy.



IDENTIFY DATA ROLES AND RESPONSIBILITIES

Understanding who is accountable for good data governance and management within directorates is key to successfully implementing good data practices and helps improve the consistency of our data governance and management across government.

We identify data roles and responsibilities through these steps:

1. Support all staff and executives to know their role and responsibilities in working with data.
2. Ensure **data custodians** and **data stewards** actively govern or manage datasets assigned to them.
3. Appoint an **Executive Data Lead** or ensure the function is assigned to an existing executive role.
4. Support the Executive Data Lead to uplift data practice and build a data culture in the directorate.

By default, all ACT Government staff are **data users** and are responsible for their own safe and appropriate use of data. Some staff have additional functions with responsibility for good data governance and management, including **data custodians**, **data stewards**, **system owners** and directorate **Executive Data Leads** (or **chief data officers**).

Directorates also carry other functions that contribute to good data governance and management, including privacy, data and ICT security and records management.

Data Providers

As data users, we have a responsibility to safely manage the data we hold and use on behalf of the community and those who provide the data to us. Data ownership is a complex issue and data collected or held by government does not grant ownership or proprietary rights, except in limited cases. We must always be aware of our responsibilities to protect personal or sensitive information and to use it for community benefit. Personal information may relate to an individual, household, business or other entity and is subject to a range of protections under privacy and portfolio legislation.

Data Users (all ACT Government staff)

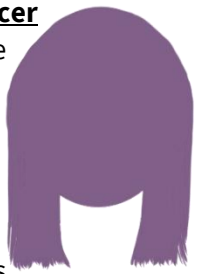
We are all data users. Using data is part of every public service role and is not solely the responsibility of data or ICT professionals. Some of us capture data as a regular part of our work, or data may be automatically generated as we perform our daily tasks using data and digital tools and systems. Data we gather might be about the people and community we serve, or about the buildings and infrastructure that we help build and maintain across the Canberra community.

As data users, we are responsible for appropriate and safe use of data in compliance with relevant policies and legislation and we are responsible for our own data learning and development.

Other data roles

A high-level overview of data roles and responsibilities is provided on the following page. The *Data Governance and Management Guide* provides more information to guide you in understanding your role and responsibilities.

Chief Digital Officer
Work with all executives and Executive Data Leads to improve data practice maturity and support a positive data culture. Responsible for data and cyber security policy. When there is a data breach, represents ACT Government in communicating to the community and works with directorates to implement a quick and effective response where required.



Senior Executive
Accountable for data decisions in their area and for ensuring that staff comply with policy and legislation. Support staff to build data skills.

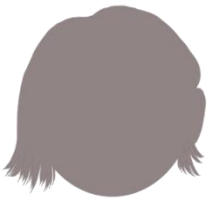
Data Custodian
Accountable for data governance decisions for datasets and authorising safe data access, use and sharing.

Executive Data Lead
Accountable for data sharing arrangements and governance decisions for all directorate datasets, establishing and implementing a directorate data strategy and fostering a positive data culture.

Agency Security Executive
Approve protective security programs for the directorate or agency.

Data Steward
Responsible for operational data management and decisions for datasets. Facilitate data access, use and sharing.

System Owner
Responsible for procurement, management, enhancement, integration and retirement of a system that hosts one or more datasets.



Privacy Officer and Records Officer
Advise data custodian, data steward and Executive Data Lead on the design and implementation of data systems and processes.

Business Owner
Ensure data systems meet business outcomes and create value for government and the community.

Data Producer
Capture and store data, and ensure the data meets the needs of the data consumer and executives.

Data Consumer
Receive data for analysis and to inform decisions.

How might data be part of our role?

Type of data use	What might this look like to you?
Accessing and reading data	Looking at information and being able to understand what it means for you, your clients and the work you are doing.
Searching records for data	Searching through various data sources to find the information you need. This may involve knowing where to go to search for data.
Analysing data to derive information and insights	Organising, examining and evaluating data to discover patterns and form conclusions. You might capture data and apply analytical and logical reasoning techniques to derive information and insights to support your work.
Making decisions based on data	Using the insights and knowledge you've uncovered through the analytical process to inform decisions.
Sharing data	Making data available to authorised users (another agency, organisation or person) in a controlled manner, such as through data sharing agreements.
De-identifying or anonymising data	Removing personal information from data to minimise the likelihood of identifying the individual the data is about.
Releasing or publishing data	Making data publicly available with no or few restrictions, including through the ACT Government's Open Data Platform or on an ACT Government website.

It is important that all these types of data use, particularly where working with sensitive or personal information, are undertaken in compliance with the legislative framework including the *Information Privacy Act* 2014 and the right to privacy under the *Human Rights Act* 2004.

BUILD A CULTURE THAT VALUES DATA AS AN ASSET

All our work to improve data governance and management practice ties back to our culture. Building a positive, proactive data culture helps us to be better prepared to work with data in safe and trusted ways. We value data in our culture and practice, and we create public value through data.

We build a culture that values data as an asset through these steps:

1	Establish and promote our shared vision, data principles and values
2	Identify barriers to achieving our data vision and embedding principles in daily practice
3	Identify and foster the desired behaviours of a data driven ACT Government
4	Measure progress towards data vision and reinforce change, and then continuously improve

The ACT Government is information-rich, with data as the raw material to solve complex policy problems and shape policy priorities, to generate targeted programs, and deliver focused and personalised services to meet community expectations.

Recent work within ACT Government has seen a shift towards data use as a cultural norm, for example through standalone teams within directorates that are responsible for managing data and leading organisation-wide data analytics, or through the data analysts and engineers in the Office of the Chief Digital Officer. Through building an ACT Government culture that *values data as an asset* to deliver community benefit, we can build our capabilities to deliver more timely and responsive services.

Workplace culture

Culture is learned and shared behaviour. It is dynamic and forever changing, influencing our everyday experiences and shaping how we view the world and engage with others and our surroundings. We transfer our cultural traits – our behaviours and practices – over time and to different settings.

Culture exists in our workplaces too: defining our environment, shared values and beliefs; the roles we play; the relationships we have with others; and how we communicate, interact and experience our day. It sets the systems, traditions and attitudes we hold at work. It helps us to identify where we belong, who we can trust and go to for support. We pass on these traits to new people who join our teams. Great workplace cultures create healthy working environments: attracting talent, driving engagement and satisfaction, and improving on our performance.

Cultural change

To create cultural change in our workplace requires a disciplined effort to understand the underlying values, beliefs and assumptions that influence how we work and interact with each other every day. It requires flexibility, time, patience and persistence. By understanding the current culture and defining the desired values, behaviours, beliefs, attitudes, systems and practices, directorates can determine the gaps between the current and desired culture, and the leadership, process, tools, and expertise needed to make and sustain the change.

Valuing data

To use data effectively and take advantage of the available data and digital systems, we need to value our data holdings. Determining the value of different types of structured and unstructured data can be a challenge in the public sector and until recently, not all directorates have viewed data as an asset to inform decisions and improve community outcomes.

The ACT Government is exploring how it might calculate the value of data, by measuring the number of times data is shared and reused, the information and insights it provides and the decisions it informed. The marginal cost of data is reduced every time it can be reused. When data stops being accessed and reused, its value decreases.

What does *valuing data as an asset* mean?

In the public sector, data becomes a valued asset when transformed from its raw state into useful and targeted insights for the fundamental purpose of informing decisions that benefit the community.

We recognise data as an asset when we:

- consistently use data to improve decisions;
- safely use, reuse and share data;
- measure the benefits generated by data;
- make staff accountable for managing data;
- define data assets and register them in an inventory or catalogue;
- safely share data with authorised users;
- build staff capabilities to realise the inherent value of data;
- release data on the open data platform; and
- quantify the financial value for high value data assets (as if on a balance sheet).

Data culture

A data culture depends on a collective and shared set of values, attitudes, beliefs and behaviour about using data. A data-driven ACT Government culture means:

- staff in all directorates and at all levels make a conscious and consistent choice to use data in every decision we make on behalf of the ACT community;
- we believe data is necessary for our work, and recognise the need to improve data capabilities;
- we are inquisitive, bold, and curious, and tell compelling data stories;
- our executives lead by example through championing and using data to shape tactics and strategies, rather than relying on experience or instinct; and
- our executives and leaders value, demand and invest in data and evidence.

These steps will help us to build an ACTPS data culture where we *value data as an asset*:

1. Define the desired data culture	Embed our ACT data vision and data governance and management principles • understand how a strong data culture will benefit service users and boost our value proposition to the community; • reflect on the ACT data principles and establish our data values; and • define what makes a strong data-driven culture and the role you and all staff play in creating it.
2. Understand the existing culture	Understand how data is currently used within the directorate: • Identify and assess current directorate data culture, its strengths and weaknesses; • determine what needs to improve inside our directorate culture to bring about change in data use to inform decisions and practice; • identify the gap between the current and future desired culture; • identify directorate data leaders and opportunities; and • prepare stories on why change will support our work and our community.
3. Establish priorities and cultural change journey	Establish the priorities that will help us evolve to value data as an asset: • identify change leadership activities and build on cultural strengths; • identify small- and large-scale shifts in behaviour and mindset - identify the behaviours we want to see and behaviours that are no longer desired; • identify our activities and functions that will help us take a more data-driven and digital-first approach in our day to day; • identify data roles and responsibilities across the directorate; and • measure and monitor progress and change.

4. Reinforce cultural change	How we communicate, communicate, communicate the change • promote shared vision, data principles and values; • celebrate desired data behaviours and call out undesirable behaviours • tell our stories and champion a data culture; • recognise soft and technical skills and proven capability; and • reward data forerunners, leaders and change makers.

Additional resources to build a data culture are found in the *Data Governance and Management Guide*.

PART II
A MANAGED DATA PRACTICE

This section provides the foundational steps that will collectively build our data maturity where staff work with data to drive trust and improve community outcomes.

- Make data discoverable
- Make data understood
- Improve data sharing
- Ensure quality data
- Make data safe and secure

MAKE DATA DISCOVERABLE

At a simple level, making data discoverable means making the data asset visible in a safe and secure way, enabling a high-level understanding of the data captured, protected, shared and used in the directorate. Data discovery (sometimes called indexing) means listing the dataset on a searchable database or register so that staff can find it. The dataset itself does not need to be accessed at this stage.

Why make data discoverable?

To access and use data, we need visibility of our data assets. Often, staff do not know what data exists, or where to go to find and access the data we need to help solve policy questions or support service delivery. Finding data can also be like looking for a needle in a haystack. With no consistent and easy way of searching for ACT Government data holdings staff may: spend time looking for data in the wrong places and not finding it; duplicating effort; or (worse still) not use data in their work at all.

How do we make data discoverable?

1	Set up data roles, responsibilities, and governance	Data custodians, data stewards, Executive Data Leads and data governance groups are accountable for overseeing data governance, management and use, including ensuring that appropriate steps are taken to make data discoverable.
2	Identify directorate datasets	Establish the datasets held by each directorate starting with the most critical, as some directorates will have a significant number of datasets including some that may no longer be active or essential. Datasets might be in different formats and different systems, from excel spreadsheets to online databases.
3	Identify, appoint and train data custodians and data stewards	Data custodians (accountable for datasets) and data stewards (responsible for datasets) make data discoverable by describing the dataset (such as the name, location) and are the key contact point for data users seeking access.
4	Register datasets in a data catalogue	Data custodians or data stewards register or list datasets somewhere that is searchable, ideally a centrally accessible hub or repository. The data itself may not be stored in a central location, but the information *about* the data should be centrally accessible. We should be able to identify that a dataset exists, even if we cannot access the data itself.

On its own, a dataset name is not enough for staff to access the data or establish whether the data will support their work. We also need to know the following:

- where the dataset is stored (e.g. the system and directorate where the data is held);
- the key contacts for the dataset (e.g. the data custodian and data steward);
- the purpose of the dataset; and
- any restrictions on accessing, using or sharing the dataset.

Addition information that may improve discoverability includes how data was captured and where it originates, whether it was purchased, who can access it and a link to the data itself.

MAKE DATA UNDERSTOOD

At a basic level, making data understood means describing the data in enough detail that data users know how, when and why the data was captured (origin), why it is used (usage) and what it is made up of (format). This can also include information about whether the data can be shared and accessed, and if it can be used for purposes other than its primary purpose. Making data understood reduces the risk of data being mis-understood, mis-interpreted and mis-used.

Why make data understood?

Data needs to be described so we know what data we have, what the data is about, understand its context and purpose, and can find it easily when we need to. Without this information, we cannot successfully manage our data or make the most of our data assets to deliver better outcomes for our community.

Making our data understood also means we can better manage the safety and security of our data, including responding better to data breaches, through quickly identifying data that is private or sensitive and providing clear information about data sharing controls and release requirements.

Metadata

The descriptive data that makes data understood is called metadata. It provides a common language about the data we use and might include title, author, registration number, data created or received, subject matter and format. We use metadata to know whether data is suitable for our purpose and how to use it.

Further information about metadata, including minimum metadata sets, is found in the *Data Governance and Management Guide*.

How do we make data understood?

1	Prepare business glossary for a dataset	Data custodians and stewards define the data using ordinary operational or business language so that it can be easily understood by staff and users. For example, what do we mean by 'customer', 'regulation', 'school' or 'appointment'? The scope of the glossary should be agency or directorate-wide where possible for consistency.
2	Prepare data dictionary for a dataset	Data custodians and stewards prepare technical definitions for each dataset, including details such as data type, permissible length and permissible domains (values). This metadata helps data analysts and other data users understand how to join, query, interpret and report on the data.
3	Identify primary use of the data	This may include identifying requirements such as informed consent and whether this was received when the data was captured. It enables data users to assess acceptable secondary uses of the data.
4	Outline data sharing rules for the dataset	Data custodians and stewards help data users know whether the data can be accessed or shared through outlining high-level controls and/or restrictions on access, sharing, using or releasing the data.

IMPROVE DATA SHARING

The ACT Government is committed to safely sharing, reusing and releasing public sector data to benefit the community while remaining transparent and accountable. To achieve this, we foster a culture that promotes safe and trusted data sharing in accordance with relevant legislation and policy.

We improve data sharing through these steps:

1	Foster a safe data sharing culture
2	Understand the risks, barriers and challenges to data sharing and release
3	Understand the legislative and policy frameworks that govern data sharing
4	Establish clear and consistent governance and management practice to enable safe data sharing, including by adopting the Five Safes data sharing principles
5	Improve open data by safely releasing more ACT Government datasets on data.act.gov.au

Put simply, data sharing means making information or data "available to another agency, organisation or person under agreed conditions"[3] and where authorised. In an ACT Government context, this might mean sharing data within and between directorates, with other jurisdictions and with non-government organisations providing services on behalf of the government. As data users, we are responsible for sharing and using data in a way that benefits the community, while ensuring appropriate protections are in place to minimise the likelihood of privacy or security breaches.

Data sharing can occur on a systematic or ad hoc basis, but always under agreed conditions established through considering the kind of data (e.g. de-identified or identifiable); relevant legislation and policy; and any privacy, security, freedom of information (FOI) or records management issues.

To share data, we must meet certain conditions in an often complex legislative and policy environment. This includes having authorisation to share data, which includes two aspects: authorised by legislation, and authorised by the data custodian accountable for the data. The data custodian's assessment and authorisation should be based on the Five Safes data sharing principles.

Data sharing is different to **open data**. 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. Open data is publicly available data that can be freely used, reused and redistributed by anyone. The ACT provides open data to the community to support economic growth, improve service delivery and achieve policy impact.

Closed data	Shared data	Open data
Data shared with authorised users on secure networks. Can include unit-record level, identifiable data.	Data shared with authorised users under specific controls and conditions. Can include unit-record level, deidentified data.	Data released for public access and can be freely used, reused and distributed by anyone. De-identified data.

[3] Office of the National Data Commissioner (2019), *Best Practice Guide to Applying Data Sharing Principles*, available from <https://www.pmc.gov.au/resource-centre/public-data/data-sharing-principles>

Why improve data sharing?

We already share data for a range of purposes, including to:

- plan, design and deliver government policies and programs based on the best available insights;
- conduct monitoring and evaluations or support compliance and reporting measures; and
- conduct and support targeted research to benefit the lives and wellbeing of the ACT community.

By improving information and data sharing alongside improvements to data governance, we can benefit the Canberra community through facilitating:

- greater community wellbeing through better services, planning, policy and research;
- improved trust in government use and protection of data and information;
- streamlined and efficient public services, delivered in more convenient and tailored ways;
- improved identification and timely services for Canberrans with diverse and complex needs; and
- increased economic activity, competition, growth and productivity.

How do we improve data sharing?

There are several existing barriers and challenges to data sharing, including a risk averse culture, a complex legislative environment, inconsistent governance and policies and outdated digital infrastructure. These are outlined in more detail in the 'understand the ACT policy, legislation and risk context' section of the Framework.

Our data sharing arrangements should consider the following five areas, supported by good data governance and management practices presented in this Framework:

Legislation	Staff and decision makers have a sound understanding of what data can be shared under the relevant legislation and are supported by data custodians who provide clear and consistent advice.
Strong governance, policy and guidelines	Directorates establish data sharing approaches supported by "data sharing by default" policies and strategies that embed the ACT data governance and management principles and the Five Safes data sharing principles. Directorates use data sharing agreements as a key tool for safe and effective data sharing.
Strong data culture	Directorates foster a data sharing culture championed by executive leaders. Staff with specific data roles, such as data custodians and Executive Data Leads, are accountable and responsible for leading this change within their directorate, including through building effective data management practices and data literacy.
Digital infrastructure	Directorates and ACT Government as a whole build and enhance technology that applies a 'data- and privacy-by design' approach so that digital systems available to all staff enable safe data sharing that protects privacy.
Strategic partnerships	Directorate executives, including Executive Data Leads and data custodians, are responsible for building strong strategic partnerships to leverage the lessons, experience, skills and knowledge of other organisations or jurisdictions.

Sharing data safely

We need to balance the value and the risk of data sharing in order to share data safely. The ACT Government has adopted the **Five Safes** as a framework to support safe data sharing, building on the

Australian Office of the National Data Commissioner (ONDC) adaptation of the Five Safes for its Data Sharing Principles.[4] Embedding the Five Safes will support us to establish clear and consistent governance and management practice to enable safe data sharing.

The Five Safes Data Sharing Principles are outlined below. Typical data sharing risks and mitigations are discussed in detail through a Five Safes lens in the *Data Governance and Management Guide*.

1. Project – *How is the data being used? Who benefits?*
Data is shared for an appropriate purpose that delivers a public benefit. Ensures data is being shared for the right reasons and outcomes, is legally valid and that there are no ethical or consent concerns.
2. People – *Who is using the data?*
The user has the appropriate authority to access the data. Guides thinking about what types of people should have access (skills, experience and qualifications).
3. Setting – *Where is the data being used?*
The environment in which the data is shared minimises the risk of unauthorised use or disclosure. Considers how data is accessed (e.g. secure lab or other environment) and controls to put in place.
4. Data – *Are appropriate protections in place?*
Appropriate and proportionate protections are applied to the data. Considers data treatments that might be needed, particularly to avoid disclosure of sensitive information, e.g. aggregate data fields.
5. Output – *How are the results of the project used?*
The output from data sharing is appropriately safeguarded before further sharing or release.

Improving open data and data release

The *Open Data Policy*, released in 2016, supports economic growth and community wellbeing. Through this policy, the ACT Government commits to making its data holdings open, following careful consideration of privacy and security and a rigorous assessment process to determine the suitability of the data for publication. The ACT open data portal (www.data.act.gov.au) hosts a wide range of datasets. The ACT Data Analytics Centre (ACTDAC) supports directorates to explore what data can be opened to the public.

Government data is shared and released in multiple formats and via multiple mediums. However, for data to be considered 'open', it must be easily accessible and published in electronic machine-readable format under a Creative Commons 4.0 International licence that permits anyone, anywhere to find, access, use, share and reuse the data for any purpose. It must have descriptive metadata associated with it.

Open data enables us to:

- improve public confidence and trust in government;
- support and grow our local economy; and
- create new knowledge and insights through research.

The *Data Governance and Management Guide* includes a detailed list of benefits of open data.

[4] ONDC 2019, https://www.datacommissioner.gov.au/sites/default/files/2019-08/data-sharing-principles-best-practice-guide-15-mar-2019.pdf

ENSURE QUALITY DATA

To make decisions using data, we need to know whether the data is fit for its intended purpose. Quality data is accurate and reliable, complete, relevant and can be trusted. We ensure quality data by knowing and improving quality issues and communicating to data users about data quality.

Why ensure quality data?

Quality data enables us to deliver better outcomes through evidence-based decision-making, while inaccurate, incomplete or misleading data risks inaccurate analysis or misinterpretation. Through improving data quality, fixing issues and communicating data quality to data users we can:

- **enable data users to trust data** to inform decisions and to use it with confidence;
- **reduce the risks** of poor outcomes for our community, harm to the government's reputation and erosion of community trust in government; and
- **improve data analytics capability** through more consistency and comparability across datasets.

Data can be used and provide value even if it is not high quality, provided staff understand the quality of the data they are using or can identify quality issues so they can be fixed.

How do we ensure quality data?

1	Adopt a data quality framework and standard	Executive Data Leads and data custodians adopt a directorate-wide data quality framework and methodology to inform the directorate's data quality practice. This contributes to building a culture that commits to quality data from the outset. All staff capture and manage directorate data using the chosen standards.
2	Identify and document data quality issues	Data custodians identify data quality issues in the datasets they are accountable for by assessing the data against the quality standards in the data quality framework. Document in a data quality register whether high value datasets conform to chosen standards.
3	Improve data quality and resolve issues	Data custodians and stewards take a proactive approach to monitor and manage data quality, including through establishing data quality improvement plans to resolve issues identified in high value datasets. In a culture that values data, quality issues are more likely to be noticed, acknowledged and addressed in a timely way.
4	Communicate issues and steps to improve data quality	Data custodians and data stewards are responsible for the ongoing process of monitoring, reporting and communicating data quality issues as they are discovered and resolved. This involves updating the data issues register and communicating openly with data users (both past and present), governance bodies and the Executive Data Lead.
5	Ensure staff have skills and capabilities to use data	Data custodians and data stewards are responsible for ensuring that data users have the skills and qualifications to use and analyse data. Even with quality data, we cannot achieve reliable, trusted or useful results if staff lack the appropriate skills for quality analytical work.

Data quality frameworks and standards

Directorates can adopt a range of existing data quality frameworks and standards. A list is provided in the *Data Governance and Management Guide*. Examples of quality standard elements are provided below:

Accuracy	The data correctly represents 'real-life' entities. Can be measured by comparison to a data source that has been verified as accurate.
Completeness	All data is present, for example, the dataset contains all the records expected and they are populated correctly.
Consistency	Data values are consistently represented within a dataset and between datasets, and consistently associated across datasets.
Integrity	The dataset is not corrupted and does not have missing or lost data.
Reasonability	The data pattern meets expectations based on what is known about the data. For example, based on a comparison with benchmark data.
Timeliness	Data is current and represents the most up-to-date version of the information.
Uniqueness	Entities are not duplicated within a dataset.
Validity	Data values are consistent with a defined domain of values, e.g. a reference table.

To support trusted use of data, we should:

- use a range of high-quality data and evidence rather than relying on a single study;
- be aware of the quality variations within datasets; and
- assess the quality of methodological approaches (was the data capture method rigorous, valid, reliable and objective?).

MAKE DATA SAFE AND SECURE

The ACT Government is committed to ensuring the data and information that we hold on behalf of the community is managed and governed in a way that keeps it safe, secure and reliable throughout its lifecycle.

We make data safe and secure through these steps:

1	Establish safe data practices, technology and controls
2	Build trust in government through safe data use
3	Support staff to know their responsibilities to implement records, privacy and security by design.
4	Establish directorate-level data protection, including a data breach response plan

The ACT Government is improving how it employs new and emerging data and digital technologies to deliver more accessible, responsive and personalised services for our community. With greater use, reuse, sharing and integration of data comes the need to build and maintain the community's trust in our ability to competently manage data while protecting personal information and safeguarding privacy.

This framework specifically identifies the preservation of privacy and the security of personal and sensitive data as a core principle. Whether we are collecting data to provide Canberrans with the services they need every day, working with data to inform policy planning, releasing data on open data or building secure information and data sharing capabilities, ACT Government directorates are obligated to maintain the safety, security and privacy of data in our activities.

SAFE	Making data safe means protecting the privacy and safety of the people the data is about. It is about removing data that is sensitive or that could identify individuals.
SECURE	Making data secure means ensuring data is protected from unauthorised access, harm (corruption) or loss (deletion) while remaining accessible to authorised users. It is about the controls we put in place around the systems in which the data is kept.

Why make data safe and secure?

Some of the data we use to inform our decisions and deliver better outcomes for our community can be sensitive and personal. This might be information that can identify an individual such as details about their gender, age, where they live, personal characteristics and lived experiences. In order to use this data, we have an obligation to act with care and attention and have proactive protections, including having systems and processes in place to ensure it is safe and secure when it is shared.

By making data safe and secure we can help prevent harm to our community by protecting the privacy and security of their personal information and protect it from being misused or unlawfully or inappropriately accessed or disclosed.

We earn and maintain our community's trust in government data use through adhering to the four Trust Principles developed by the Australian Data and Digital Council:

Respectful	Secure	Accountable	Transparent
Act fairly and ethically Make engaging with us easy and listen to your views	Protect your privacy Implement strong security systems	Be honest about mistakes and learn from them Respond quickly when things go wrong	Proactively communicate with you Where safe to do so, provide data openly to the public

How do we make data safe and secure?

Making data safe and secure should be a feature in everything we do, and all directorates must establish appropriate measures to safeguard individual privacy.

We use a 'records, privacy and security by design' approach to data across the entire lifecycle: when we capture, store and use data, when we share or release it for broader access, and when we archive or destroy it.

All staff are responsible for making data safe and secure, but some roles, such as Executive Data Leads, data custodians, records officers and ICT staff, have additional responsibilities, such as building a 'privacy aware' culture, ensuring business systems protect personal data and identifying learning opportunities for staff.

Privacy and Security risks evolve over time and so too should our responses. Further information about how we make data safe and secure, including examples of tools and activities, is provided in the *Data Governance and Management Guide*.

Proactive and Responsive Data Breach Practice

A data breach occurs when personal information or protected information held by the ACT Government is subject to unauthorised access or disclosure or is inappropriately lost or accessed. It may also be called a 'data security incident' or 'privacy breach'. Section 12 of the *Information Privacy Act 2014* (ACT) defines a privacy breach as 'an act or practice that breaches a Territory Privacy Principle (TPP).'[5]

Data breaches can occur even when we are vigilant and proactive about how we work with data. They can range in size and may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems. For example:

- loss or theft of physical devices (e.g. laptops) or paper records containing personal information;
- unauthorised access to personal information by an employee;
- disclosure of personal information due to 'human error' (e.g. an email sent to the wrong person) or as a result of inadequate identity verification procedures (e.g. to a scammer);
- incorrect configuration of access controls, meaning data is exposed to unauthorised users; and
- download of personal information from data storage to insecure mediums such as shared drives.

Directorate data breach response plans

Executive Data Leads are responsible for proactively preparing directorate data breach response plans before an incident occurs. Plans should be flexible given the broad range of possible incidents, and be

[5] The Territory Privacy Principles (TPPs) are based on the Australian Privacy Principles (APPs). The TPPs outline how personal information is handled, the uses of personal information over time and that the principles may be applied across different technologies.

designed collaboratively with data custodians, data stewards, executives, privacy officers, chief information officers, Shared Services ICT Security and the whole of government Chief Digital Officer.

The ACT Government applies the OAIC's data breach advice, which includes the following steps:

Data breach	Staff, contractors or external party alert directorate to suspected or actual breach.
Staff member or contractor	Immediately notify line manager, executive and data custodian about the breach. Record time and date of the breach, type of information involved and context, cause and extent of the breach.
Executive	Determine whether a breach has or may have occurred. Determine if the data breach and its potential impact requires escalation to the data breach response team, notify Executive Data Lead and privacy officer.
Data breach response team	Directorate privacy officer establishes data breach response team, including data custodian and steward, Shared Services ICT Security and Executive Data Lead. 1. Contain the breach 2. Assess the risk for individuals and take steps to remediate risk of harm 3. Consider who must be notified 4. Review incident and take action to prevent future breaches.
Executive Data Lead	Evaluate how the data breach occurred and the success of the response to help improve future data handling and data breach management in the directorate and across ACT Government.

Engage with the community

To build and maintain public trust in our use of data, we must be open and transparent about how we use data and protect personal information, and we must proactively engage with the community including in responding to privacy concerns. In the event of a significant data breach, the Chief Digital Officer is responsible for communicating to the community on behalf of the ACT Government.

PART III
A MODEL TO MEASURE DATA MATURITY

MEASURE DATA GOVERNANCE AND MANAGEMENT CAPABILITIES

Our data strategies will help identify the present state of our data effort and define the way we will implement the previous 11 steps to improve data practice. For example, in some directorates datasets exist in file structures and systems, with low visibility and sharing. Over time, we will to transition from a state of ad hoc and inconsistent management to a mature state where data is consistently discoverable, understood, governed, shared, high quality, and safe and secure. The following five levels can be used to assess our data governance and management maturity: Initiate; Develop; Define; Manage; and Optimise.

	Level 1 Initiate	**Level 2 Develop**	**Level 3 Define**	**Level 4 Manage**	**Level 5 Optimise**
	Disorganised and ad hoc	Being developed	Standardised and communicated	Managed and measured	Continuously improving
PART I – A DATA-DRIVEN CULTURE					
Establish Directorate Data Vision and Purpose	Undeveloped and not shared across Directorate	Directorate data vision is established	Directorate data vision is shared and embedded in strategies and plans.	Directorate data vision is seen in behaviours and executives review progress.	Unified Directorate data vision and data assets are continually enhanced.
Know the ACT Policy, Legislation and Risk Context	Poor or inconsistent awareness and understanding of data experiences, risks and barriers.	Establishing context for data practice, privacy and security including barriers to achieving the data vision.	Clarity of data risks and data practice including data and information sharing.	Executive actively manage data risks.	Unified understanding and application of data practice to manage and mitigate risks.
Know the ACT Data Principles	Inconsistent models in handling and using data.	ACT Data Principles acknowledged.	ACT Data Principles defined for day to day practice.	ACT Data Principles are present in day to day behaviours.	Unified set data principles across all data assets and practice.
Establish Directorate Data Governance	Undeveloped, and/or inconsistent data governance in directorate structures.	Directorate data governance structures established.	Directorate data governance bodies oversee data policy and practice.	Data Governance is embedded in Directorate structures and processes.	Ongoing feedback loops to enhance directorate data governance arrangements.
Identify Data Roles and Responsibilities	Ad hoc and unsupported data capabilities and literacy.	Data capabilities defined and supported; executive data lead appointed.	Data roles assigned to every dataset and active data capabilities program	Staff routinely build data capabilities and positions describe data specific roles.	Ongoing feedback loops to enhance data capabilities, roles and responsibilities.
Establish A Culture That Values Data as an Asset	Undeveloped, not shared, and/or inconsistent data culture.	Desired data culture is being identified and existing barriers to data culture identified.	Data culture is defined in directorate strategy and leaders commit to change journeys.	Data culture is embedded in day to day behaviours.	Unified data culture. Subject to review & improvement.
PART II – A MANAGED AND MATURE DATA PRACTICE					
Make Data Discoverable	Data is in silos, disorganised & poor visibility.	Datasets are being identified and registered.	High value datasets are findable and accessible.	Management actively engaged in data discoverability.	Datasets maintained, updated and publicised.
Make Data Understood	Ad hoc and unsupported data documentation.	Dataset documentation processes being established.	High value datasets described, and new datasets are defined at capture.	Dataset described in machine-readable format and data is modelled against an enterprise data model.	Continual improvement of data definition processes & capabilities.
Improve Data Sharing	Data is accessible only to a small group or locked down.	Data sharing (Five Safes principles) arrangements being developed.	Well defined data sharing arrangements and facilities.	Data routinely shared using five safes data sharing principles and agreements.	Continual improvement and communication of data sharing infrastructure.
Ensure Quality Data	Data quality is ad-hoc. and the potential for reusability is limited.	Data quality framework and standards are established / adopted.	Data quality issues defined.	Data quality issues are managed for high-value datasets.	Continual improvements of data quality system.
Make Data Safe and Secure	Data is stored in ad-hoc facilities.	Data security facilities and data security standards are being established.	Dataset is held in a system with well-defined data security and storage facilities.	Data routinely managed in secured repositories.	Continual improvements of data security and safety systems

GLOSSARY

The following terms are used throughout this framework. A more detailed glossary, including technical terms, is provided in the *Data Governance and Management Guide*.

DATA	
Administrative data	Information collected for delivering public administration, e.g. for registration, transaction and record-keeping.
Business glossary	Simpler version of data dictionary, defining terms relating to a dataset in ordinary business language clearly understood across directorate (business-facing definitions).
Data	Observations and measurements of things that we are interested and care about. Based on the facts, observations, images, computer program results, recordings, measurements or experiences on which an argument, theory, test or hypothesis, or other activity or output rests. Generated, collected, acquired or used during projects or public service operations, and in some cases may include the output itself. May be numerical (quantitative), descriptive (qualitative), visual or tactile. It may be raw, cleaned or processed, and may be held in any format or media.
Data capture	Systematic recording of data. Once captured, organised and evaluated, data becomes information. When data and information are analysed and interpreted in the context of the organisation, the key lines of inquiry or questions, and in relation to other factors and variables, they become evidence.
Data dictionary	Document comprising the technical definitions and metadata information of all fields in a dataset.
Dataset (or data set)	Structured collection of data, that is stored, published or curated in a single source, available for authorised access or download in one or more formats. Lists values for each of the variables for each member of the dataset. Can consist of a collection of data, documents or files. A dataset in tabular forum includes columns representing a variable and each row corresponding to a given record.
Dataset register	A list of all known datasets to provide visibility, discoverability and access to authorised users. Can be a simple list such as in shareable document, or a SharePoint site or data catalogue.
Master data	Core dataset that is essential to government operations.
Metadata	'Data about data', a set of information or facts about the data in the dataset(s) for the purpose of attribution, description, management, verification and discovery.
Quality standards	Set of criteria used to measure data quality.
Structured data	Organised data that is generated by people, such as when data is inputted into a computer in spreadsheets and databases (e.g. name, age, post code, gender), and by machines such as Sensory Data (GPS data, street sensors, Bluetooth devices, medical devices), Point-of-Sale data (credit card information, product information),

	call detail records (time of call, caller information) and web server logs (page requests).
Unstructured data	Information that either does not have a pre-defined data model and/or is not organised in a predefined manner. Forms of unstructured data include social media, text files (e.g. word documents, PDF documents, books, letters, other written documents, audio and video transcripts), audio files (e.g. customer service recordings, voicemails), presentations (e.g. PowerPoint), videos (CCTV, personal video, YouTube), images (e.g. photographs, illustrations, memes), messaging (e.g. instant messages, text messages).
DATA USERS	
Authorised user	Someone assessed by a data custodian, including through the application of the Five Safes data sharing principles, as being authorised to access and use data for an agreed and authorised purpose, especially data that may include personal, confidential and/or sensitive information.
Data custodian	Typically a senior executive or manager, accountable for data governance decisions for all internal and external datasets assigned to them.
Data owner (also known as data provider)	Individual, household, business or other entity that provides data to a government agency or has data about them supplied by a third party
Data steward	An officer or manager responsible for operational data management and decisions for all internal and external datasets assigned to them.
DATA SHARING AND OPEN DATA	
Data release	Making data publicly available with no or few restrictions on who may access the data and what they may do with it.
Data sharing	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.
Data sharing agreement	A formal arrangement between a data custodian and another agency, organisation or individual that details conditions under which data is shared and used.
Open data	Publicly available data that can be freely used, reused and redistributed by anyone without restriction.
DATA SAFETY AND SECURITY	
Data protections	Changes made to data to minimise the likelihood of identifying the data provider.
De-identified data	Data relating to a specific individual where personally identifying details and unique characteristics have been removed to prevent identification of that individual. Also known as anonymised data.
Non-sensitive data	Data that is anonymised and does not identify an individual or breach privacy or security requirements.

Personal information	Also known as personally identifiable information or PII, this Framework uses 'personal information'. The *Information Privacy Act 2014* defines personal information as "information or an opinion about an identified individual, or an individual who is reasonably identifiable— (i) whether the information or opinion is true or not; and (ii) whether the information or opinion is recorded in a material form or not; but (b) does not include personal health information about the individual."
Sensitive information or data	The Office of the Australian Information Commissioner defines Sensitive Information as a subset of personal information, or an opinion (that is also personal information) about an individual's: racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information about an individual, genetic information (that is not otherwise health information), biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or biometric templates. Other forms of sensitive data can include confidential data such as commercial in confidence information and research data, and ecological data that may place vulnerable species at risk. The Office of the National Data Commissioner identifies *Particularly Sensitive Data* as any data where unauthorised disclosure would likely lead to adverse consequences for the individual, agency, organisation or Australia in general. Data which is of a personal, legal, commercial, security or environmental nature may be considered particularly sensitive. This is broader than the *Privacy Act 1988* definition of sensitive data which is defined as a subset of personal information and limits how it can be collected and used.

Data Governance and Management Policy Framework

August 2020

ACT Government