Australian Government
Department of Finance

APS Data Ethics Framework

2024

Contents

Introduction 1

- Purpose 1
- Aims 1
- Scope and application 1

TRI data ethics principles 2

- Transparency 2
- Respect 3
- Integrity 4

Identifying and monitoring ethical risks 5

- Data ethics risk indentification 5
- Example risks related to transparency 6
- Example risks related to respect 6
- Example risks related to integrity 7

Roles and responsibilities 8

- Data ethics RACI 11

© Commonwealth of Australia 2024

With the exception of the Commonwealth Coat of Arms and where otherwise noted, this product is provided under a Creative Commons Attribution 4.0 International Licence. (**http://creativecommons.org/licenses/by/4.0/legalcode**)

The Australian Government have tried to make the information in this product as accurate as possible. However, it does not guarantee that the information is totally accurate or complete. Therefore, you should not solely rely on this information when making a commercial decision.

The Australian Government is committed to providing web accessible content wherever possible.

If you are having difficulties with accessing this document, please email: **datapolicy2@finance.gov.au**.

Version: 1.0

Introduction

Purpose

The Data Ethics Framework provides guidance on the ethical use of data and analytics (D&A) in the Australian Public Service (APS). This framework applies to government activities involving D&A, including where artificial intelligence (AI) is used in analytics, and contributes to fostering and maintaining public trust in Government's use of data and analytics.

Aims

The ethical use of D&A is foundational for well-informed design and delivery of policy, programs, and services. The importance of ethical use of D&A is part of the vision of the **Data and Digital Government Strategy**, which aims to 'deliver simple, secure and connected public services, for all people and business, through world class data and digital capabilities.' Building and maintaining public trust in Government's use of D&A requires clear and practical ethical principles, APS wide collaboration, and a shared understanding of capabilities required to embed the Framework.

This Framework provides a common language and set of expectations for the ethical use of D&A.

> Data ethics is defined as that which guides the use of D&A in a manner that has transparency, respect and integrity throughout the lifecycle of D&A use.

> Use of D&A covers a spectrum of activities, including creating and deriving data as well as collection, storage, access, analytics (inclusive of AI and generative AI), automation, sharing, re-use, transformation, aggregation, integration, migration, archiving and disposal of data.

Scope and application

This Framework may be useful for agencies regardless of whether they already have established ethical frameworks for the use of D&A in place or not. This Framework is not intended to override existing agency policies and frameworks. It is a voluntary framework that can be used to support existing practices within agencies.

Depending on their specific circumstances (including data roles and existing D&A policies), agencies should consider:

- how this Framework should be integrated with their role in providing policy, programs, and/or service
- how staff should apply the Framework
- the potential impacts of perceived or actual misuse of D&A (whether intentional or otherwise) for their agency and the APS as a whole.

The Framework should be read in conjunction with relevant enabling legislation and policies as it applies to specific agencies. These legislation and policies may prescribe the application of processes (including ethics processes), which take precedence over this Framework. Section 2, Principles, provides general exemplars of relevant legislation and policy.

TRI data ethics principles



The TRI Data Ethics Principles of **Transparency**, **Respect** and **Integrity** underpin the practical application of the Framework. The principles apply to the full spectrum of D&A activities. An agency's actions, behaviour, culture, and decision-making should be guided by the application of these principles. The clear and consistent application of the principles will increase public trust and confidence in Government use of D&A.

Where D&A activities involve AI, these principles should be read with reference to **Australia's AI Ethics Framework**, which informed the development of the principles. This may be particularly relevant for concepts related to contestability of decisions.

Transparency



- Our data collection and use have a clear purpose.
- We are open about the decisions and actions we take with D&A.
- We can trace the lineage of D&A decisions and actions, including maintaining explainability (e.g. understanding how data is used, how outputs and decisions were arrived at) of how we use data and analytics.

Transparency is a cornerstone for fostering public trust in data use. Transparency should be considered in a way that is meaningful and appropriately contextualised for relevant audiences.

Achieving transparency from an ethical perspective requires the holistic consideration of D&A use within the setting of an agency's policies, programs, and services, and with respect to the objectives that have given rise to the use of data. Maintaining explainability of analytics activities is essential for achieving transparency. This includes appropriately documenting D&A use and may also include use of technological tools for complex systems. Acting in a transparent manner includes the following actions.

We are committed to **following best practice guides and standards for documenting and communicating how we use D&A** to administer projects, programs, and services.

We are proactive in **maintaining explainability of our analytics activities**, including using appropriate tools and technologies to establish and maintain explainability of AI, automation, and complex analytics systems. As complexity of our analytics increases, we maintain focus on explaining how these systems work and assuring the accuracy, integrity, and oversight of the outputs of these systems.

We can **justify the ongoing relevance of data collection and use** throughout the lifecycle of D&A uses, including clearly articulating how the D&A use aligns with the goals of the program, policy and/or service delivery and with the agency strategy.

We **have** a **mechanism for assessing, documenting, and communicating when data should be archived or destroyed** as part of our D&A activities. We are aware of our obligations under relevant legislation, including archival legislation.

We **ensure D&A use and outputs are secure, auditable, and replicable**, and where appropriate should include provisions for notification of individuals affected by the collection, sharing, and use of data.

We ensure that **appropriate controls are documented and in place** for the D&A use. We recognise the importance of having a human in the loop when developing and implementing controls. We recognise that these controls must stand up to scrutiny, especially for higher risk D&A uses, and be able to be produced and communicated in a clear and understandable way. This may be especially important for processes that involve analytics, such as model development, AI or processes involving automated decision making.

We have a **clear and open process to explain when elements of these principles cannot be satisfied** and can provide this justification to relevant stakeholders as required.

We are **proactive with** the **identification and management of ethical requirements, procedures, risks and issues** associated with D&A use, and can communicate these in a meaningful way to appropriate stakeholders to ensure risks are understood at the appropriate levels.

We **periodically review measures for** ensuring **transparency**, including mechanisms for maintaining explainability.

We have mechanisms for **sharing D&A outputs** when and where it is appropriate to do so.

Respect



- We genuinely consider, engage and/or partner with those likely to be affected by our data decisions.
- We put fairness for individuals and groups at the center of our data decisions and actions. We make decisions about D&A that are inclusive and for the public good.
- We manage bias in our data collection and use, and mitigate its potential impact on decision making.

Respect is essential for guiding how we use D&A and the impacts of data use. Acting with respect means striving for fair and equitable outcomes, and includes the following actions.

We **consider the impact on individuals, groups or entities** affected by D&A use. We do so at the earliest opportunity when planning to use D&A. Where there are potentially significant impacts, we are proactive in addressing these and engaging in discussion and consultation about these impacts where it is practical and appropriate to do so.

We have clear processes to **resolve competing interests fairly** in situations where individuals, groups or entities are not aligned in relation to the use of data in D&A activities, including data sharing.

We have mechanisms in place to **manage situations where legislation authorises D&A use**, but doing so is inconsistent with one or more of the Data Ethics Framework principles. These situations are managed with consideration for impact on individuals, organisations and/or groups.

We **consider social and economic impacts at commencement of D&A use**, including a process that weighs the public good and against the impacts on those affected, so that this weighting is clearly understood, acknowledged, and managed as appropriate.

We **consider the potential for biases in D&A use** and have measures in place to assess and manage these risks. These risks may be especially pronounced for projects or work that involve legacy systems, AI or automated decision making.

We **maintain visibility of the public's sentiment** towards our D&A use and this informs our decision making around new and/or continued use of D&A activities.

Integrity



- We ensure D&A is used appropriately, consistent with the purpose and legal authority for which it was collected and intended.
- We comply with Australian legislation, regulations and the Privacy Principles.
- We maintain appropriate expertise and practice stewardship (e.g. oversight and management) of our D&A activities.

Integrity is at the heart of ethical conduct. Acting with integrity means recognising and maintaining our individual accountabilities for D&A across a range of uses, and acting in line with the **APS Code of Conduct**. Acting with integrity also means maintaining the integrity and accuracy of data we collect, derive and use in our D&A activities, and meeting our obligations under the **Privacy Act 1988** and the **Privacy (Australian Government Agencies – Governance) APP Code 2017**. It includes the following actions.

We **only proceed with D&A use when it is lawful**, and we have adequate protections in place to monitor the impacts of our D&A use on individuals, groups or entities.

We undertake to **only collect and use** D&A **where it is reasonably necessary for, or directly related to, our agency's functions and activities**. This includes regularly reviewing agency's business need for D&A to ensure it remains aligned with agency, Government, and community expectations.

We **maintain an understanding of the authorising and regulatory environment**, and we recognise our obligations to comply with relevant laws, policies, and other requirements relating to D&A use.

We undertake to **consult early and regularly with relevant experts** when in doubt about the authorising and regulatory environment, including with agency's own legal service and compliance areas.

We undertake to **ensure the data we use is gathered from reliable, reputable and verifiable sources**.

We **periodically review the reliability and quality of the data and analytics** outputs throughout the lifecycle of D&A use, regardless of the system, tool or product used, including AI.

We ensure **appropriate stewardship of D&A use** by considering its role in improving processes and considering the long-term impacts of its use on the individuals, groups, and entities represented by the data.

We undertake, where appropriate, to **consult with individuals, community groups and relevant entities** who will be **affected by D&A use**, including decisions made through D&A use. This includes partnering with affected individuals, groups and entities to co-design policies, programs, and services that ensure the protection of their data, where there is no security impediment to doing so.

When making decisions, we ensure the **balance of benefit and harm** does not result in obtaining benefits for a majority at the cost of harm to other individuals, groups or entities. This includes balancing what functions agencies are required to perform with how agencies perform those functions. Where relevant, we adhere to relevant NHMRC polices and the AIATSIS Code.

Identifying and monitoring ethical risks

Identification of ethical risks and issues in D&A use is the first step in managing its potential impact. The following steps may be employed to surface, discuss and address ethical risks.

Step 1: Ensure there is a clearly defined scope and purpose for D&A use and that this relates to a policy, program or service. Using D&A without a clear relationship to such functions raises the risk of inappropriate use.

Step 2: Identify and understand potential ethical risks through assessing D&A use against the Framework Principles.

Step 3: Engage and consult, including impacted stakeholders and internal ethics committees and experts as appropriate.

Step 4: Develop a plan to manage ethical risks and maintain transparency with impacted parties.

Step 5: Implement plan to manage ethical risks.

Step 6: Monitor and review for changes in D&A use and associated changes in identified risks. Key changes may include: changes internally to D&A use; external changes such as a shift in policy, program, or service; changes in the legislative or regulatory environment; change in tools; changes in community expectations on how the Government uses D&A. Responsibilities for monitoring and review should be defined and documented.

Data ethics risk indentification

To identify potential ethical risks, agencies may assess their D&A use against the principles. Where agencies do not have a D&A ethics assessment process in place, this may be achieved by interrogating whether a D&A use is in line (where appropriate) with the action statements under each principle. Making this assessment should be done with careful consideration to preconceptions and potential for harm. Agencies should recognise different types of D&A may have different risks. Secondary use of D&A, using data directly to take actions (especially through AI and automation), and using data about diverse, vulnerable or protected groups may elevate the risk of its use. The following considerations may also raise the level of data ethics risk:

- no or ambiguous consent in the absence of a legal mechanism
- no clear understanding of the potential for bias in the data collected
- a disregard for, or lack of confidentiality, when managing D&A
- poor or undocumented D&A management practices (e.g. no mechanisms to monitor for unintended consequences)
- no identified steward for the D&A activity
- limited understanding of data collection relevance to a function or intent of data collection
- taking advantage of socially vulnerable groups, whether this be actual or perceived
- limited or disingenuous stakeholder engagement and collaboration
- no clear understanding of the provenance of the data, including whether it was generated through AI.

The following tables provide some examples of risk consequence according to each principle. These are indicative only, providing an indication of the kinds and levels of risk you may encounter. Examples may relate to more than one principle.

Example risks related to transparency

Risk consequence	Example
Low risk	There is a clearly defined and documented purpose for the collection and use of D&A which is endorsed by key stakeholders, and this purpose is in line with the Agency administering its core functions. There is a clear and documented process for destroying data, and this is supported by assurance activities and accepted accountabilities for data use.
Medium risk	There is a defined purpose for the collection and use of D&A, but this purpose and its relationship to the Agency's core functions is not documented and there is no documentation of endorsement by key stakeholders. There is a process for destroying data, but this is not documented, assurance is not sought, and it is not supported by accepted accountabilities for data use.
High risk	There is no specified purpose for the collection and use of D&A, and it is loosely related to the Agency's core functions. There is no process for destroying data, and limited accountability for data use.

Example risks related to respect

Risk consequence	Example
Low risk	There are robust processes in place to identify bias within the data and its use in analytics, and there is a clear strategy for mitigating bias. These biases are clearly documented so that future users of the data and subsequent analytics (including their outputs) are aware and can implement mitigations as appropriate. A clear, consistent, and documented approach to resolving conflicts is in place, this pathway to resolution is delegated to the appropriate SES level, and there is appropriate representation in the group for the issues being resolved.
Medium risk	Processes are in place to identify bias, but these and their mitigations are not documented. There is limited information about biases captured to inform appropriate on-use of the D&A. There is a documented path for resolving issues which has appropriate representation and SES delegation, but this has not been tested.
High risk	No bias checking is in place and no mitigations for bias have been identified. There is no documentation related to bias to inform appropriate on-use of D&A. There is no path to issue resolution, or the path is not at the appropriate SES delegation and does not have appropriate representation.

Example risks related to integrity

Risk consequence	Example
Low risk	There are clearly defined, and documented roles and responsibilities related to the D&A activities, and the individuals who have specific roles and responsibilities acknowledge these in writing. The data is collected and used in analytical solutions that clearly meets end user needs and improves the Agency's delivery of core functions. This can be evidenced by supporting documentation (e.g. scoping papers).
Medium risk	There is an understanding of roles and responsibilities related to the D&A activities that are acknowledged by the individuals who hold these roles/responsibilities, but there is no documentation or formal acceptance of these. The data is collected and used in analytical solutions that meets end user needs and improves the Agency's delivery of core functions, but there is minimal documentation or supporting evidence.
High risk	There are no defined roles and responsibilities in place for the D&A activities. There is no or limited evidence that the data collection or analytics solution meets the end users' needs and improves the Agency's delivery of core functions.

Identifying and managing ethical risks should be informed and supported by an agency's internal risk management practices. This includes assessments of overall risk rating based on the likelihood of ethical risk occurring. Agencies may find as their level of D&A maturity grows (including but not limited to data ethics, data management, stewardship of D&A), this maturity will act as a control for ethical risks discussed in this Framework.

Roles and responsibilities

Using D&A ethically is everyone's responsibility. It is essential for meeting and upholding the standards the Australian community expects from us in line with the **APS Code of Conduct**. This section outlines four key roles and responsibilities associated with the application of this framework.

As a	Ethics Advisory Group/Committee
I am in this role if I am a...	SES band 2 or 3 (or equivalent) member of a decision-making group such as an audit and risk committee, information or D&A governance committee, strategy or technology committee. **Note**: this may be supported by external ethical review bodies or groups.
Responsibility statement	Ethics Advisory Groups/Committees already embedded into your agency should be used to provide expert advice on the use of D&A for specific projects or activities within the agency. As a member of an Advisory Group or Committee you should: • provide guidance and advice on the use of D&A for specific projects or activities in the agency • be a point of issue escalation for ethical risks • draw from personal and networked experience for professional opinions or specialist advice • ensure ethics is considered as an integral part of new projects or processes • review and provide support and guidance to agency staff where data ethics risks or issues are raised • utilise the agency's information governance framework and enterprise-wide information management strategy • understand the strategic vision and how the Data Ethics Framework principals align to agency practices.

As a	Senior data leader
I am in this role if I am a...	Chief Data Officer, Chief Data and Analytics Officer or senior executive officer with similar responsibilities. **Note**: this role may be aligned with: • the accountable officer role in the Policy for the responsible use of AI in Government. • accountabilities and responsibilities for senior SES in data roles outlined in ***SES Accountabilities for Data***.

Responsibility statement	Australian Government senior data leaders are responsible for their agency's governance and use of data as an asset, as well as maturing their data capabilities. As a senior data leader, you should undertake the following to support ethical data and analytical use: • ensure the agency has an agency-level mechanism(s) for managing ethical risks and considerations related to D&A use, including consideration of D&A ethics in the use of AI and other analytics and automation technologies • set the criteria for escalating ethical issues and risks • build and maintain public trust in your organisation's use of D&A by adhering to a standard for data ethics • ensure compliance with relevant legislation and information management policies • ensure appropriate stewardship of D&A.

As a	**Branch, business line or division executive**
I am in this role if I am a...	SES Band 2 (or delegated Band 1) who is accountable for D&A projects **Note**: this role may be aligned with accountabilities and responsibilities for all SES officers as outlined in ***SES Accountabilities for Data***.
Responsibility statement	Branch, business line or division executives have responsibility to ensure ethical principles are applied when agencies collect, use, integrate and analyse data assets. As the accountable executive, you should: • ensure assessments of ethical risks are undertaken for D&A projects • be accountable for ethical risks that arise from D&A projects • act as a champion to ensure the operational application of D&A ethics • ensure others understand their ethical responsibilities and best practices that align to your agency policies and procedures • escalate ethical risks above tolerances to appropriate authorities such as senior data leader or advisory groups/committees • raise awareness of ethical issues and alignment to Government expectations to drive lasting change • ensure requests for access/use of owned data assets are approved only when the intended use complies to your agencies agreed ethical standards • ensure data quality, privacy, safe access, discoverability, ethical sharing, and use arrangements, including use of appropriate metadata • manage information with integrity • understand specific risks associated with tools, system or processes, including AI, and ensuring mitigations are in place and monitored.

As a	Data professional
I am in this role if I am a...	Staff using data to inform or drive their work, staff using the analytics solution or the data product being built, such as business line subject matter experts and data analysts or scientists. Executive level staff member responsible for managing or delivering work that involves D&A use. Some examples may include data analysts, data engineers or data scientists; data managers; geospatial analysts or statisticians; policy, program or product owners; delivery or record managers; or privacy or FOI officers.
Responsibility statement	Data professionals have specific responsibilities as front-line developers, users of D&A, or end users of a data product. The use of D&A must be managed in accordance with your agencies agreed ethical standards, considering potential ethical risks. Data professionals should: • identify ethical risks, including through assessing ethical risks associated with D&A use • inform SES of the ethical risks associated with D&A use • ensure the application of ethical principles regardless of tool, product or process used, including AI, processes involving automated decision making, and/or other analytics solutions • understand how the data asset has been collected and under what authority, including consent • maintain awareness of other available references to support understanding of ethical considerations and mitigations • protect data assets during the collection, use and analysis of data, specifically where sensitive or personal information is used • critically examine D&A solutions to identify and mitigate any potential negative data bias • ensure analytics and their outputs are interpretable and explainable to maintain transparency • understand the potential wider societal impact of D&A use, including perceived risks for disproportionate targeting of groups • undertake appropriate training in new technologies before application to data assets • ensure that sharing, or publication of D&A outputs adheres to the legislative instrument for which it was collected and captured • manage information with integrity and consider how D&A may be reused • maintain the quality and accuracy of the data sets and analytics solutions being used in products your agency owns or manages.

Data ethics RACI

This RACI provides, at a high level, some of the key products and activities that should be used to ensure application and accountability of ethical practises are forefront in agency considerations when using D&A.

Ethics Practice	Advisory Groups/ Committees	Senior data leader	Branch/ business line division executive	Data professional
Implementing agency level D&A ethics governance	Informed	Accountable	Consulted	-
Undertaking an assessment of the ethical risks associated with D&A use	Informed / Accountable	Informed / Accountable	Informed / Accountable	Responsible
Applying the Framework to D&A projects and activities	Informed	Accountable	Consulted / Responsible	Responsible
Quality and accuracy maintenance of artefacts related to D&A ethics	-	Accountable	Responsible	Consulted
Periodically checking that the application of the Framework is in line with legislative instruments	Responsible	Accountable	Consulted	Informed