Data Strategy & Governance
26 May 2022

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA
CREATE CHANGE

Enterprise Data Ethics Framework

Metadata for document management

Version	1.0
Approval Authority	University Senior Executive Team
Document Custodian	Chief Information Officer
Last Approval Date	26 May 2022
Next Review Date	April 2024
Audience / Users	UQ all
Information Security Classification	OFFICIAL-PUBLIC
Author	Trinity McNicol, Business Analyst—Data Strategy and Governance
Notes	

Contents

1. Purpose

The Enterprise Data Ethics Framework (the Framework) provides a consistent enterprise-wide approach for the ethical use of data for non-research purposes across The University of Queensland (UQ).

This document outlines seven Ethical Principles that apply to activities that collect, generate, or otherwise utilise data.

1.1 Scope

The Framework applies to all staff who work with data at UQ. All activities that collect or use new or existing data for non-research purposes fall within scope. Data within both the *Corporate* and *Teaching & Learning* areas is in scope for this Framework. Please note that this is not limited to personally identifying information (PII) or other information of a sensitive or confidential nature, as all data may have ethical considerations. For more information about data at UQ, including Information Domains[1], please refer to the Data at UQ website.

For all matters relating to research ethics, please refer to Research Ethics and Integrity.

1.2 Supporting documentation

The Framework should be read in conjunction with the following policies, procedures, and information:

1.50.01 Code of Conduct

1.60.02 Privacy Management

6.40.01 Information Management Policy

6.40.02 Information Security Classification

6.40.03 Data Handling

6.40.04 Destruction of Records

6.40.05 Access to UQ Documents

UQ Right to Information and Privacy

Information Governance and Management Framework

Enterprise Data Ethics Handbook

Data Ethics Assessment Tool

Relevant legislative obligations are highlighted in these documents.

[1] An Information Domain is a broad category or theme under which University information can be identified and managed. UQ uses the Topics and Entities outlined in the CAUDIT Higher Education Data Reference Model, in the context of business capabilities and organisation structures, as a guide to determine appropriate information domains.

2. Ethical Principles

Ethics help us navigate the space between what can be done under legislation and policy, and what we should do morally. Considering how we work with data through an ethical lens helps mitigate risk for both individuals and the University. Potential ethical issues should be considered at all stages throughout the Information Lifecycle – from initial collection, to how data is stored, used, shared, archived, and disposed of.

The following Principles support decision-making when working with data, providing a consistent standard for how we use data ethically at UQ.

Principle 1: Purpose of data use must be defined, and balance benefits and harms for data subjects and stakeholders.

When using data, the purpose and any proposed interventions or actions should be clearly defined upfront. Expected benefits and harms for data subjects and stakeholders should be identified. Benefits should be balanced to address the power imbalance between the organisation and data subjects.

Principle 2: Transparency is key, and engagement with stakeholders fosters trust.

The intent for the use of data should be clearly communicated with data subjects and stakeholders, along with information about how the data will be used, linked with other datasets, and any interventions that may be implemented based on insights obtained from analysis. Information presented to data subjects should be in an easily accessible format, using language that can be clearly understood by the average person. Data subjects should be able to review and update data about them, and provide feedback on data uses that directly affect them. A culture of trust should be fostered between the organisation and data subjects, with clear communication a foundation for this relationship.

Principle 3: Informed consent must be obtained for collection and use of data

For consent to be informed, data subjects must be aware of what data is collected, how it will be used, and any interventions that will result. Information should be detailed enough for data subjects to understand the breadth and variety of data that will be collected and potential uses, without being so prescriptive that future uses will be out of scope. Consent should be actively managed. Renewal of consent will be required when the scope of work materially differs from what was disclosed at the time consent was originally obtained. Data subjects should be given the opportunity to opt out of having their data collected or used. However, opting out may carry consequences which data subjects and those using the data should be informed of.

Principle 4: Strategies should be implemented to minimise harm and reduce bias.

An assessment should be conducted to consider potential harms that may arise from the collection, use and storage of data, or interventions resulting from analytics insights. The potential for bias should be minimised where possible, through thorough consideration of data quality, data selection, assumptions, analytical processes, and evaluation of subconscious bias. Data science activities such as machine learning and artificial intelligence require further scrutiny due to their potential to amplify underlying bias.

Principle 5: Data subjects' right to privacy must be respected

Privacy is a fundamental right and should be respected. The collection, storage and use of data should implement a "privacy by design" approach to ensure that only data that is truly required is collected, stored appropriately, used in a manner that respects the individuals' rights to privacy, with access rights appropriately managed. To respect the right of data subjects to be forgotten, metadata should allow for the identification of all data pertaining to a given individual, including new datasets created as part of an analytical process, or captured in a downstream system.

Principle 6: Legislation should be considered a minimum requirement for appropriate data use.

Data collection, storage, use, archival, and destruction must be done in accordance with relevant legislation, policies and procedures. However, this should be considered a minimum requirement. Those using data should have the appropriate knowledge and skills for the work they are conducting, statistical models should be sound, and data should be of sufficient quality for the application. Those responsible for and working with data should have sufficient data literacy and training for the role they are undertaking.

Principle 7: UQ and individuals are accountable for the ethical use of data

Everyone has a role to play in ensuring data is used ethically. While UQ is ultimately accountable for the ethical use of data, Information Stewards are responsible for managing data-related conflicts, risks and issues and approving appropriate uses. Individuals should also be held accountable for the responsible and ethical use of data in their day-to-day work activities. Information Stewards, Information Consumers, and Information Creators must be supported in their decision-making process when considering the ethical implications data-driven activities. Individual use cases may be referred to the Ethics Advisory Group for consideration in situations where further guidance is desired.

3. Applying the Ethical Principles

Ethical decision-making is a risk mitigation strategy. The Ethical Principles defined in Section 2, along with the Data Ethics Risk Assessment Tool, support individuals working with data to consider the risks and impact of their work. While ethical concerns are most pertinent for personally identifiable information (PII), they should be evaluated for all data types. Principles 3 and 5 address consent and privacy respectively, and therefore are only relevant for activities where PII is used. Certain scenarios may not completely satisfy each of the Ethical Principles, and therefore may carry a higher risk.

Ensuring the correct people are responsible for making decisions about how we work with data underpins ethical practice. Under the Decision Rights Model described in the Information Governance and Management Framework, Information Stewards are responsible for the day-to-day management of data within their Information Domain, including approving access to data for Information Consumers, and provide business rules to Information Creators. It is essential that Information Stewards are aware of and satisfied with the level of risk associated with data-related activities that fall under their Information Domain.

The processes for data collection and data sharing are discussed below. Each of these processes utilises the Decision Rights Model, and highlights where the Framework is implemented to support the ethical use of data.

3.1 Process for data collection

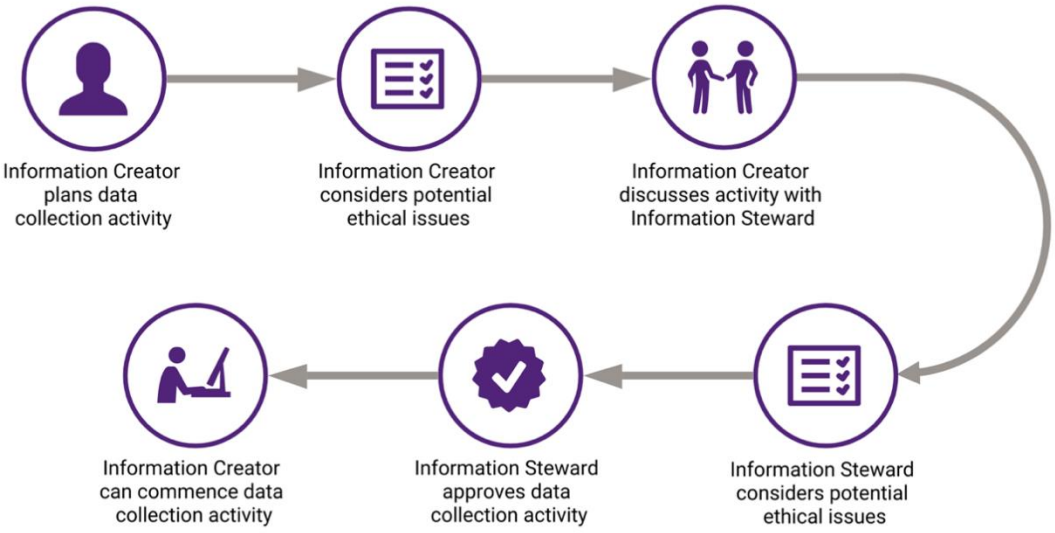

Figure 1: Key steps for ethical consideration and approval of data collection activities

Data is collected, collated and generated through a range of activities at UQ. Some of this data is collected directly from data subjects (individuals providing data about themselves) by the University. Other data is generated automatically by machine-driven processes or systems. We also obtain data from third parties, such as Government agencies.

For Information Stewards to take responsibility for all data within their Information Domain, they must be aware of what data exists. For this to happen, Information Stewards must have an active role in the planning and approval of any activities that collect or generate new data at UQ. Information Creators can liaise with the Data Strategy and Governance team to determine who the appropriate Information Steward is for a proposed dataset. It is essential that Information Creators engage with the relevant Information Steward or Stewards early when planning data collection activities.

The Ethical Principles outlined in Section 2 should be considered by Information Consumers when planning data collection activities. The Ethical Principles should also be used by Information Stewards when reviewing proposed data collection activities.

3.2 Process for data use

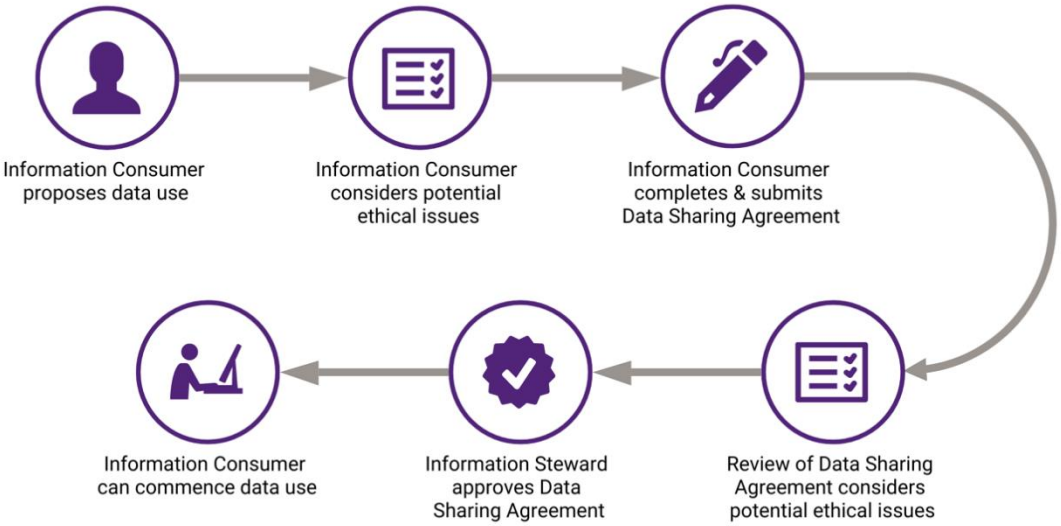

Figure 2: Key steps for ethical consideration and approval of proposed data uses

Access, sharing and reuse of non-research data at UQ is facilitated by Data Sharing Agreements. An Information Consumer must complete a Data Sharing Agreement to access corporate-owned data at UQ, with separate Data Sharing Agreements for Analytics or Integration use cases. Once submitted, the Data Strategy & Governance Team will liaise with the Information Steward to review and facilitate approval of the proposed data use.

To ensure thorough consideration of ethical issues, Information Consumers should refer to the questions in the *Privacy and Ethics* section of the Data Sharing Agreement, the Ethical Principles defined in Section 2 of the Framework, and the Data Ethics Risk Assessment Tool. The Ethical Principles also underpin the review of the Data Sharing Agreement.

In some instances, Information Consumers may wish to use data they already have access to for a purpose that has not been approved under the original Data Sharing Agreement. If the new use differs materially to the use originally approved a new Data Sharing Agreement should be submitted. This ensures appropriate oversight for how data is used at UQ, and minimises the risk of any potential ethical concerns.

3.3 Ethical considerations throughout the Information Lifecycle

Information lifecycle management is the consistent management of information from creation to final disposal. The information lifecycle at UQ includes the phases shown in the diagram below. Potential ethical issues should be considered at every phase of the information lifecycle and will vary depending on the type of data. Some possible considerations for each phase are outlined in the following sections.

Fig. 3 – Information Lifecycle Diagram

3.3.1 Plan and Design

Planning and design activities should not only be considered at the initiation of the information lifecycle, but also reviewed at every subsequent stage.

3.3.2 Create, Capture and Classify

Ethical considerations in this phase may include:

- Consideration of data sources, including if PII will be used.
- Assessment of data quality, including any limitations, assumptions, and sources of bias.

3.3.3 Store and Secure

Ethical considerations in this phase may include:

- Security requirements for where data is stored, to ensure privacy.

3.3.4 Maintain and Manage

Ethical considerations in this phase may include:

- Consideration of ethical and legislative requirements, including the Ethical Principles described in the Framework.
- Management of consent and usage rights or restrictions.
- Determining a clearly defined purpose
- Communication and transparency to ensure data subjects and stakeholders are informed about of what data is collected, stored, and used, and for what purposes.

- Engagement with data subjects and stakeholders to understand needs, perspectives and expectations.
- Consideration of benefits and potential for harm for data subjects and stakeholders when evaluating proposed data uses.

3.3.5 Share and Reuse

Ethical considerations in this phase may include:

- Management of consent and usage rights or restrictions.
- Consideration of benefits and potential for harm for data subjects and stakeholders when evaluating data access requests.
- Determining conditions for sharing data internally and/or externally to UQ.
- Deciding upon any licencing requirements or restrictions on use for published information or data.
- Consideration of risks to privacy and/or security when sharing information or data, including consideration of the mechanism for data sharing.

3.3.6 Retain and Archive

Ethical considerations in this phase may include:

- Consideration of benefits and potential for harm for data subjects and stakeholders when evaluating what information and data should be retained for archival purposes.

3.3.7 Dispose or Destroy

Ethical considerations in this phase may include:

- Consideration of benefits and potential for harm for data subjects and stakeholders when evaluating and establishing a timeline for the destruction of information or data.

3.4 Escalation to the Ethics Advisory Group

The Ethics Advisory Group reviews and provides advice on complex ethical matters, including data-related concerns. Both data collection and use activities may be referred to the Ethics Advisory Group if Information Stewards require additional support in determining if ethical risks have been appropriately mitigated.

For further information about the Ethics Advisory Group and how to submit a proposal please contact the Data Strategy and Governance team via email.

4. Roles and Responsibilities

Roles and responsibilities as relevant to this Framework are outlined below. Further roles and responsibilities are detailed in the Information Governance and Management Framework.

Information Trustee

The Information Trustee is accountable for ensuring information is protected in accordance with ethical standards.

Information Leader

An Information Leader is responsible for providing direction regarding the ethical use of information across its lifecycle, and promoting awareness and understanding of ethical data use across the University.

Information Domain Custodian

An Information Domain Custodian is responsible for defining domain specific procedures and rules to ensure ethical use of information throughout its lifecycle.

Information Steward

An Information Steward is responsible for applying the Ethical Principles when reviewing and approving (or rejecting) requests for access to data and information assets.

Information Creator

An Information Creator is responsible for complying with the Ethical Principles when capturing, generating or providing information and data.

Information Consumer

Information Consumers are responsible for the ethical use of the University's information and data assets.

Ethics Advisory Group

The Ethics Advisory Group is responsible for reviewing and providing advice on non-research data use cases referred for consideration. More information about the Ethics Advisory Group is available by contacting the Data Strategy and Governance team via email on datagovernance@uq.edu.au.

5. Further support

If additional support is required when assessing potential ethical issues, individuals can contact the Data Strategy and Governance team for advice via email on datagovernance@uq.edu.au.

6. Glossary of Terms

Consent: Consent is the process of providing permission or agreement for something to happen.

Data Ethics: The moral standards applied, and assessments made, when working with data. This extends beyond the consideration of data uses that are allowed under legislation. (Note: Data ethics requires evaluation of the risks and benefits to data subjects and stakeholders who may be impacted by the data activity, and consideration of whether the proposed data activity would be considered acceptable by these individuals.)

Data Subject: A data subject is an individual described by the data.

Data Use: Data use refers to any way data might be recorded, edited, updated, analysed, processed, aggregated, transformed, read, or otherwise processed.

Data: Raw data are individual, unorganised facts that need to be processed. Data may be structured (organised in consistent field structures and formats) or unstructured (without a pre-defined model or format).

Ethics: Ethics are the moral principles or values that guide decisions or behaviour of an individual or group.

Harm: Harm can be considered anything that is detrimental to an individual. Harm may be in the physical sense, mentally or emotionally, or to one's reputation.

Impact: To have an effect on someone or something. This may be a positive, negative or neutral effect.

Information Consumer: Information Consumers select the best source of information to meet their requirements for use.

Information Creator: Information Creators capture or create the information as defined by the Information Domain Custodian.

Information Domain Custodian: Information Domain Custodians (Information Custodian) define and implement safeguards to ensure the protection of information within their Information Domain. This must be done in accordance with the policies, procedures and rules approved by the Information Trustee or Information Leader.

Information Domain: An Information Domain is a broad category or theme under which University information can be identified and managed.

Information Leader: Information Leaders provide strategic guidance regarding information requirements within one or more information domains.

Information Steward: Information Stewards are responsible for the quality, integrity and use of the information assets within their Information Entity on a day-to-day basis. An Information Steward may manage multiple information assets. The stewards apply relevant policies, procedures and rules, including safeguarding the information from unauthorised access and abuse.

Information Entity: An Information Entity is a specific group of information that is related to an Information Domain.

Information Trustee: The Information Trustee has enterprise level authority and accountability under legislation for the collection and management of the University's information. At UQ, this is the Vice-Chancellor.

Information: Information is data that has been processed or presented in a way that provides context and meaning.

Informed consent: Informed consent is the process of providing permission or agreement for something to happen, with a thorough understanding of the context and possible consequences.

Personally identifiable information (PII): Personally identifiable information is “any information relating to an identified or identifiable natural person.”[2] It may also be referred to as personal data.

Privacy: Privacy is the right to freedom from surveillance and intrusion, and the ability to control what information you share with whom and for what purpose.

Risk: Risk is the ‘effect of uncertainty on objectives’[3], where effect is a deviation from the expected outcome. Risk may be caused by a single event or a set of circumstances that affect, adversely (threats) or beneficially (opportunities), the achievement of objectives.

[2] GDPR Article 4: Definitions
[3] ISO 31000:2018

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

Contact details

Office of the Chief Information Officer
T +61 7 3346 6881
E it-governance@uq.edu.au
W its.uq.edu.au

CRICOS Provider Number 00025B