The University Of Queensland
AUSTRALIA

CREATE CHANGE

# Enterprise Data Ethics Handbook

# About the Enterprise Data Ethics Handbook

## Purpose

**The Enterprise Data Ethics Handbook should be read in conjuction with the Enterprise Data Ethics Framework.**

This Handbook provides practical guidance to help you consider how each of the Ethical Principles from the Enterprise Data Ethics Framework (the Framework) may apply to the work you are conducting. While all data may have potential ethical concerns, only non-research data use cases are within scope of the Framework.

"The Enterprise Data Ethics Framework promotes trust and provides reassurance for the UQ community that data is used appropriately and with integrity."

*Mr Rowan Salt,*
*Chief Information Officer (Acting)*

## The importance of ethics

**Ethics help us behave in a way that is honest, accountable, fair, and respectful of others.**

Considering the ethical implications of a scenario enables us to navigate the shades of grey, particularly when actions are not clearly wrong or right.

Data ethics are the moral standards applied, and assessments made, when working with data. Just because we have the data available or capability to leverage said data to gain insight does not mean all uses are acceptable or just.

Applying ethical decision-making to how we use data enables us to move from simply questioning what we *can* do with data under policy and legislation, to what we *should* do with data.

## Some general considerations

**Ethical decision-making is a risk mitigation strategy.**

Considering potential ethical issues helps minimise risk for data subjects, data stakeholders, and The University of Queensland.

The Ethical Principles outlined in the Framework are designed to help you evaluate the range of ethical considerations that may be relevant for your proposed use of data. In certain situations, you may be unable to satisfy each of the Ethical Principles. This does not necessarily mean your proposed data use is unethical, but rather that it carries a higher potential risk for ethical concerns.

You may also find that not all of the Ethical Principles are relevant for your proposed use of data. For example, Principles 3 and 5 are specific for situations where personal data is used.

## Ethical Principles

The following seven Ethical Principles are from the Framework:

- **Principle 1:** Purpose of data use must be defined, and balance benefits and harms for data subjects and stakeholders.
- **Principle 2:** Transparency is key, and engagement with stakeholders fosters trust.
- **Principle 3:** Informed consent must be obtained for collection and use of data.
- **Principle 4:** Strategies should be implemented to minimise harm and reduce bias.
- **Principle 5:** Data subjects' right to privacy must be respected.
- **Principle 6:** Legislation should be considered a minimum requirement for appropriate data use.
- **Principle 7:** UQ and individuals are accountable for the ethical use of data.

Each of these Ethical Principles will be considered in more detail in this Handbook.

## For more information

**The Data Strategy and Governance Team within Information Technology Services can provide guidance and support on a range of data ethics matters.**

You can contact the Team via email on **datagovernance@uq.edu.au**

**The Data at UQ website provides more information about data ethics and related topics.**

View the website at:
**https://data.uq.edu.au/ethics**

**For training on Ethics, we recommend the following options:**

- *Data Ethics: What does it mean for you?* training available via **Staff Development** (online)
- *Ethics Awareness Workshop* available via **Staff Development** (in-person)

# 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.

## Establish your purpose

Determining the purpose of prior to commencing your work helps you to reflect on your intentions, establish what you are trying to understand or achieve, and decide if the work is truly necessary.

## Identify all stakeholders

Data subjects — those who are described by the data you plan to work with — are the most obvious stakeholder group when you are working with personal data. However, all types of data may have stakeholders who could be affected by or interested in your work, even if you are not working with personal data. Examples may include academics who teach within a certain course, researchers conducting research in a certain discipline, or UQ as a whole.

## Impacts for stakeholders

Once you have identified all relevant stakeholders, you should take the time to consider how each stakeholder or group may be affected. Will stakeholders be directly or indirectly impacted by how you plan to use data? Will they benefit from this work? Is there any potential for harm, either from your work or interventions that may result?

Benefits and harms can take many forms, and may not be immediately apparent. It is important to recognise that not all individuals within a larger stakeholder group may feel the same about how you plan to use data, or the interventions that might be implemented.

It is also important to consider the power imbalance between the University and data subjects when evaluating impacts.

## What if impacts aren't positive?

Impacts do not always need to be positive to be ethical. Work that has negligible impact on certain stakeholders is likely to carry a lower risk for ethical concerns. In some situations, even data uses that result in a negative outcome for a data subject may still be ethical.

# 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.

## Transparency is key

Data subjects want to know what data about them is collected by the University and how it will be used. Communication about this should be conducted in a way that is transparent and clear.

Often, any disclosure of data collection practices or potential uses are burried deep in lengthy Terms and Conditions Agreements or similar documents. Studies have shown that users either do not engage with such documentation, or struggle to decipher the legalistic language in which they are usually written. This ultimately means that many data subjects remain uninformed about how data about them is collected or used. Similarly, data stakeholders should also be made aware of how proposed uses of data may affect them.

## Engagement over communication

Engagement allows for two-way dialogue, and therefore a richer understanding of potential issues and impacts that may arise from a proposed data use.

Where practical, engaging with data subjects and stakeholders is preferable over one-way communication options. This empowers individuals who may be affected to voice any concerns they may have, raising awareness of potenital ethical issues that may otherwise have gone undetected until the proposed activity was underway.

Allowing data subjects and stakeholders to have a voice also fosters trust by demonstrating the are a respected part of the process.

# 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.

## Is consent required?

In general, consent is required any time you are collecting data from individuals, or using data for any purpose that was not disclosed at the time the data was collected. However, in specific circumstances, it may be acceptable to forgo obtaining consent. These exceptions are usually outlined in relevant policies, procedures or legislation.

## Obtaining informed consent

To consider the consent process to be truly informed, data subjects must be provided with sufficient information to understand what data about them will be collected, and how it may be used. This information should be clear and easy to understand, and specific enough so that data subjects have a reasonable expectation of all potential uses. Where possible, the consent process should also be voluntary. In certain situations data will be legally required, such as for administrative purposes. However, it may be practical to consider allowing individuals the ability to opt out of having their data used for other specific purposes.

## Management and renewal of consent

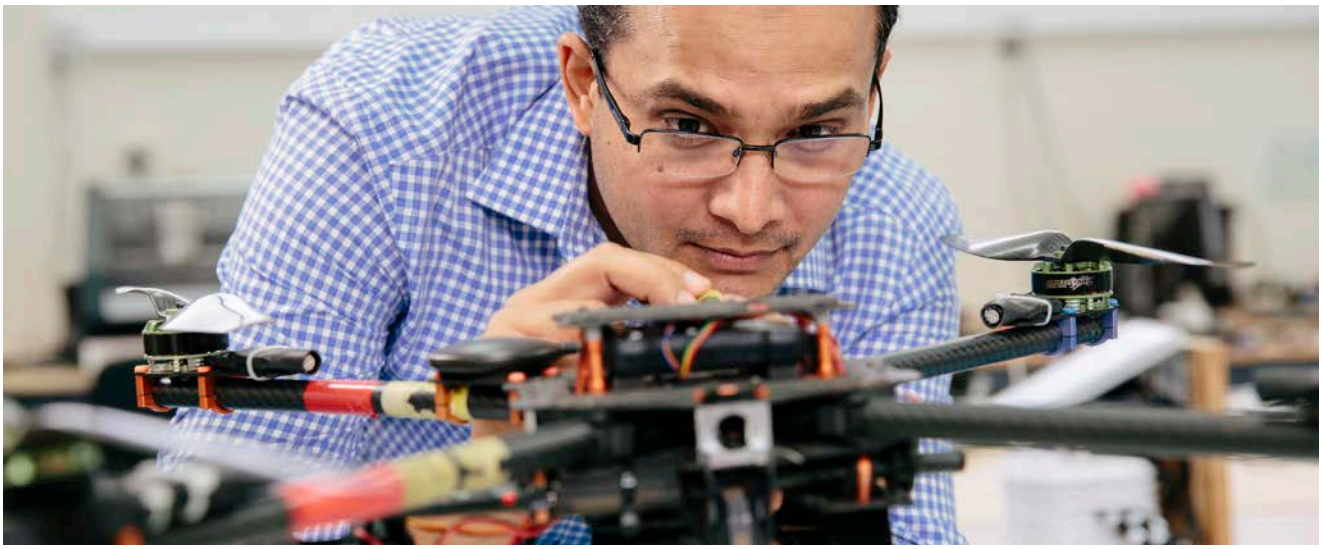
Where possible, any uses that were consented to at the time data was collected should be recorded within the relevant metadata.

Future data uses that fall out of scope of the original consent obtained may require renewal of consent. It may fall upon those using data to seek consent from data subjects for novel uses of data. Information Stewards will be able to provide guidance on when renewal of consent is required.

# 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.



## Bias is complex

Bias is a complex issue. Firstly, we all have subconscious bias we must recognise. Every individual who is involved in working with the data or acting on the insights generated should consider their own potenital biases. Being aware of our own biases and taking steps to minimise any potential impact is essential.

Bias may also be introduced or amplified by:

- data quality
- assumptions
- data selection
- data visualisation
- machine learning
- artificial intelligence (AI)
- other algorithms.

To ensure potenital sources for bias are properly addressed and do not introduce ethical concerns, thorough scruitny of the data, analytical processes and outputs is necessary.

## Predicting and detecting harm

Even when we propose a use for data with the best of intentions, it is still possible to unintentionally cause harm.

Harm can be challenging to predict. Sometimes it cannot be detected until analysis is already underway, or outputs of analysis may even indicate that harm has already taken place. The potential for harm must also be considered when insights are acted upon and interventions are introduced.

When considering the potential for harm, it is important to think of the data subjects, all relevant stakeholders, and the University. Harm may present itself in many forms, affecting wellbeing, reputation, privacy, and so forth.

Ongoing review throughout the duration of the activity utilising data is essential to ensure any evidence of harm is acted on promptly.

## Responding to evidence of harm

If harm is detected at any stage during the data use activity, it is important that this is responded to appropriately and with haste.

This can be particularly challenging in a siloed organisation such as UQ. All individuals working with the data or implementing interventions should have an understanding of the potential harms that may be observed, and how to act on these if detected. It may be necessary to liaise with the relevant Information Steward or Organisational Unit to discuss the best course of action.

# 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.

## Privacy varies between individuals

Privacy is a complex concept, and individuals will each have their own idea of what privacy means to them. This will be shaped by their belief system, values, experiences, culture and demographical factors. It is important to consider how privacy may vary within a group of data subjects or stakeholders.

## Minimising data collection and storage

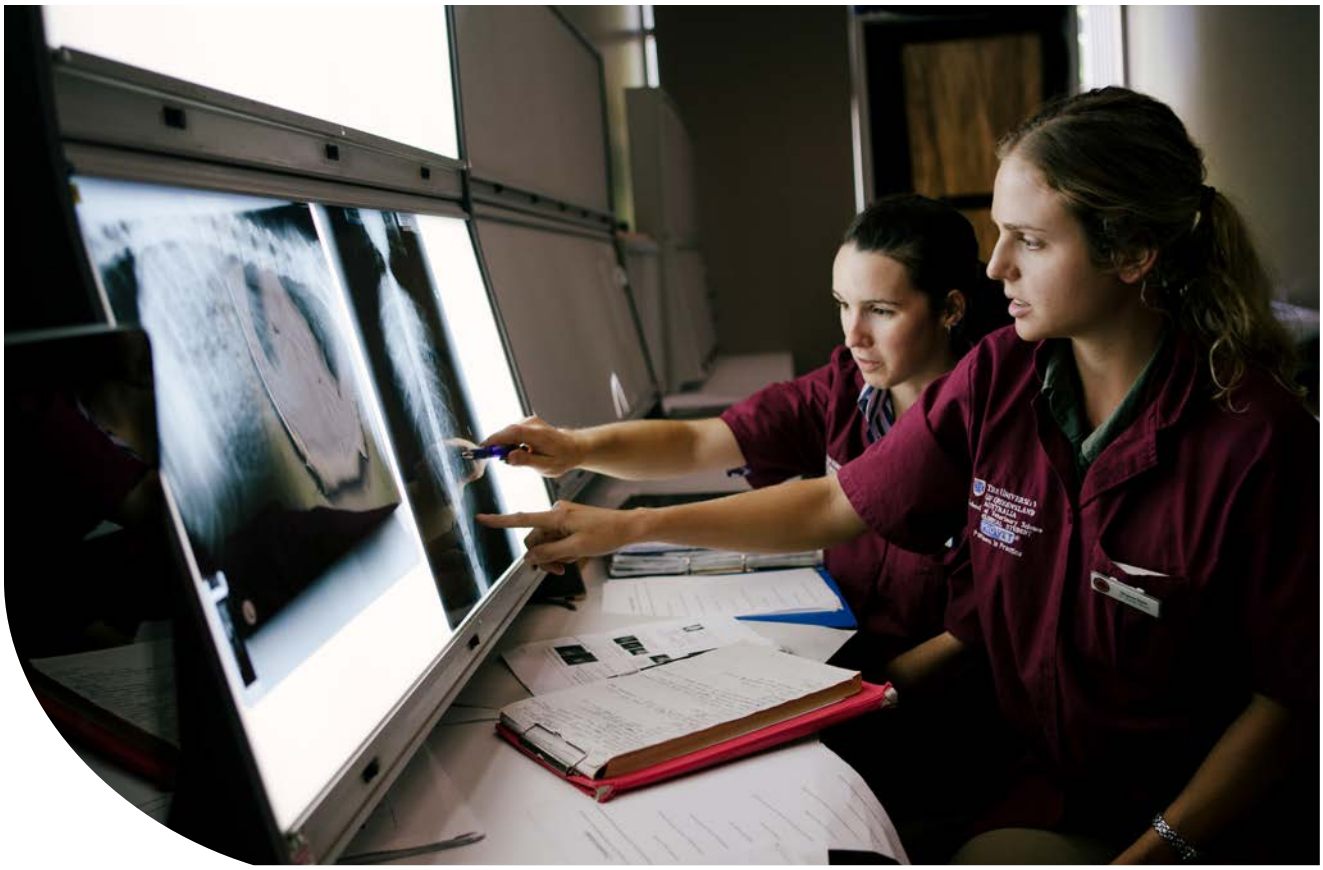
Where possible, a "privacy by design" approach should be implemented. Ideally, only data that is truly required should be collected. This data should be stored appropirately, with access tightly controlled. Data uses should respect the data subjects' right to privacy. Finally, once data is no longer required, it should be destroyed in accordance with relevant obligations under legislation and policy.

Of course, in practice this will not always be possible. Rather, effort should be made to satisfy as many as these recommendations as possible.

## The right to be forgotten

Under the European Union's General Data Protection Regulation (GDPR), data subjects have the right to request the erasure of all data that relates to them. Currently, such laws do not exist in Australia. However, there has still been much discussion around an individual's rights to be forgotten by an organisation.

Ideally, metadata should be captured and managed in a way that allows for the identification of all data pertaining to a particular individual. Practically, this is much harder to achieve.



# 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.

## Meeting legislative obligations

Appropriate use of data must meet the obligations outlined in the relevant legislation, policies and procedures. The Framework lists the relevant UQ Policies and Procedures that should be considered when working with data. In addition, each of the UQ Policies and Procedures reference the legislation that also must be adhered to. Meeting these obligations is considered the minimum standard.

## Using data in accordance with approvals

Data must only be used for purposes that are covered by existing approvals. Any additional use cases should be considered by the Information Steward to ensure the use is appropriate, respects the original context of collection, is in line with relevant legislation, policies and procedures, and is free from ethical concerns. A Data Sharing Agreement should be submitted for any use which is outside the scope of any existing approvals.

## Importance of data literacy

All work that utilises data requires some degree of data literacy. As the complexity of the work increases, so does the level of skill required. It is important that those working with data have the necessary skills and training to understand the nuances and implications of the work they are conducting. Some roles that require specific skills sets may require individuals to hold certain qualifications. Continuing professional development will also be key to ensure those working with data have up-to-date knowledge in such a rapidly evolving field.

# 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.

## Accountability relies on everyone

While ultimately the University is accountable for how data is used, everyone has a role to play.

- Information Consumers must ensure they use data appropriately, and in line with relevant approvals.
- Information Stewards are responsible for ensuring data-related conflicts, risks and issues are managed appropriately.
- Information Creators must act with integrity, ensuring information collection respects the rights of data subjects and data is handled appropriately.

Additional roles and responsibilities are outlined in the Framework.

## Support for ethical data use

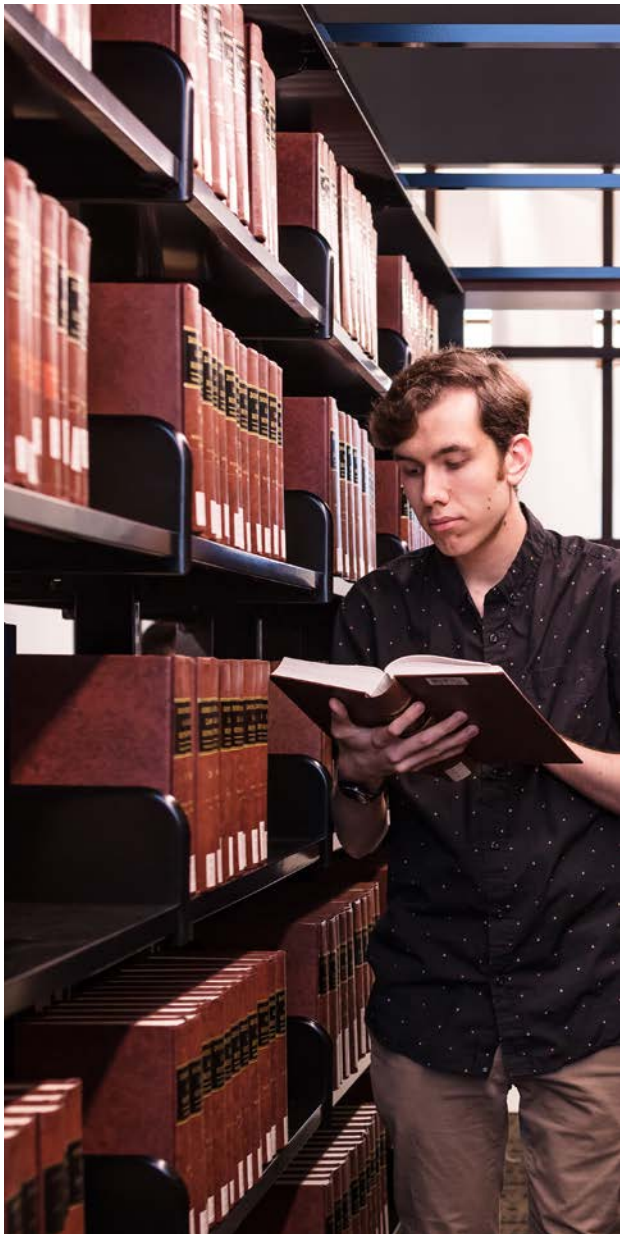
Regardless of how you are working with data, there is support available to help you navigate any ethical dilemmas you you may face.

You can access the Framework and general supporting information on the Data at UQ website. In addition, the Data Ethics Risk Assessment Tool is also available to help identify potential ethical risks associated with a proposed data use.

Regular data ethics training sessions are also available. These are delivered online. More information about these sessions can be found on the Staff Development website.

For particularly challenging ethical dilemmas, Information Stewards may elect to refer proposed data use cases to the Ethics Advisory Group. This group has been established to provide advice on complex ethical matters. Referrals are facilitated by the Data Strategy and Governance team.

Finally, the Data Strategy and Governance team are always happy to provide individual support. They can be contacted directly via email.



**Data Strategy & Governance**
Information Technology Services
Email: datagovernance@uq.edu.au
Web: data.uq.edu.au

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

CRICOS Provider 00025B