

Personal privacy considerations are one of the ways in which the ethical principles around personal information are addressed in the design and conduct of human research. It is the responsibility of researchers to have due regard for the privacy of participants.

Privacy needs to be considered from both a statutory, compliance and ethical viewpoint. The Privacy Act 2020 is the framework within which we are guided from a statutory perspective. This document will detail different considerations which you must consider for your research.

Privacy relates to the personal information of living individuals. "Personal Information" is defined as:

any information which is related to an identified or identifiable person e.g., name, date of birth, contact details, student/staff ID.

The University of Canterbury also has its own Privacy Obligations. An up-to-date overview of Privacy policies, declarations, and other standards can be found on the Privacy Obligations page here: [Privacy and Official Information | University of Canterbury](#).

A good "rule of thumb" when considering privacy is always 'would I want this to happen with my personal information?'. Put the individual at the centre of your thinking, rather than thinking about the information as a "data set".

A researcher demonstrating care around an individual's Privacy can be beneficial, and may:

- Increase the likelihood an individual will choose to participate in a project.
- Increase the candour of the information participants provide for a project – as participants are not worried about who can access and what is happening with their information.
- Decrease the likelihood of complaints or concerns about their information's use in the research.
-

The Privacy Act 2020 governs how organisations and businesses can collect, store, use, and share personal information. The Act ensures that:

- You know when your information is being collected.
- Your information is used and shared appropriately.
- Your information is kept safe and secure.
- You can get access to your information.

The Act is a principles-based document, with 13 Information Privacy Principles (IPPs) which you should consider when dealing with private information. Further information about these principles is detailed in [Appendix 1](#).

There are also Privacy “Codes of Practice” that detail specific privacy rules for personal information in six specific areas. The main one to be aware of for research with human participants is the Health Information Privacy Code 2020, which can be found here: [Office of the Privacy Commissioner | Health Information Privacy Code 2020](#). If you are doing research in the field of health, please ensure that you are familiar with the heightened requirements around managing health information.

Personal Information held overseas If you are moving/sharing personal information across countries (e.g. when working with international academics), please ensure that you are aware of any additional requirements around data sharing and transfer which may differ by region and country. Information Privacy Principle 12 (IPP 12) states that personal information transferred overseas must be adequately protected. The Office of the Privacy Commissioner has a decision tree tool to help you with this [here](#). This will also help you with contract clauses, if required.

Researchers have important ethical and regulatory responsibilities when designing, conducting, and reporting human research. These responsibilities apply to all human research, irrespective of the design, discipline, academic level, or funding source.

In summary, when conducting research, you must:

- Only collect, access, and use identifiable personal information that is necessary for the research – if you don’t need it, don’t collect it.
- Obtain consent or waiver of the consent requirement to collect, access, and use personal information.
- Be aware of the sensitivity of the research and how it may impact the participant to engage with the project in terms of both their personal safety and ongoing wellbeing.
- Handle identifiable information responsibly (including safeguarding against unauthorised access to the information).
- Not disclose personal information to third parties.

Privacy is an important component of ensuring ethical recruitment of participants for your research. Just because you have access to contact information for other purposes does not automatically allow you to use this to recruit participants. For example, you may have access to tutorial lists, attendance records, or academic results as part of your professional employment. This does not mean you can access these for your research, either directly, or for the purposes of recruitment.

Initial contact with potential participants must consider:

- The degree to which other parties (e.g., ~~Á Z v μ U %a en(loyer)~~ employer) will know whether the individual has been approached about their participation, and the degree to which this could then expose them to risk (for example: social, physical, economic, or legal risk).
- The degree to which potential participants might consider an approach from a researcher about a project to be a form of invasion of their privacy.

It is important to recognise that power dynamics potentially come into play during recruitment activities. For example, if one person has a degree of power over the potential participant, this can put subtle or unintended pressure on them to feel like they have to say “yes” to participating (e.g., an employer whom they may rely on for references, or a lecturer who assesses their work).

It may be prudent, depending on the project, for the recruitment and consent process to clarify whether others will know the participatory status of individuals.

Please see the [Human Research Ethics Policy](#) for more information.

I will not be publishing/reporting identifiable personal information...so do the privacy principles still apply to my research

There is a common misconception that, so long as a researcher protects the privacy of their participants when they publish/report the outcomes of the research, privacy regulations do not apply to that research. This is incorrect.

If a researcher will access, collect, generate, or otherwise obtain identifiable personal information, privacy regulations apply to that research even if the individuals will not be named or otherwise identified in any publications or reports arising from the research.

Additional privacy principles will also apply if the data will be analysed, stored, reported, and/or shared with others in an identifiable form.

Researchers may want to use student-related data held by the University, and in some cases the researcher already has access to this data. Using student data for internal (i.e., School/Departmental) analysis is allowed (for example, teaching/learning and process improvements). This is covered under the [UC Privacy Declaration](#). However, this authorised use does not cover research projects for external publication. A prospective research project (potentially for publication) would require an ethics application and provision of informed consent by students for the use of the relevant data.

For retrospective use of historical data, a case-by-case approach is taken. Generally, such cases are not likely to receive ethical approval, as the information would not have been originally gathered for research purposes. If you wish to use historical student data in your research, an ethics application is required, and the following should be considered:

- Is the data still available?
- If student outputs (assessment data etc.) could possibly identify the student (whether intentionally or not), this will require the researcher to seek consent from each student.
- Only data from students who have consented would be able to be used.
- No identifiable data from students could be used without their consent.

In any research, it must be clear to participants from the outset whether they will be anonymous (unable to be identified) or identified. Depending on the research it may be appropriate for participants to be identified and their contributions acknowledged, or it may be that if they are identifiable this will make them vulnerable or expose them to some other risk. It must also be clear to participants that they can make an informed decision about their participation. Consent must be clear, informed, and given prior to the proposed research taking place, with any ethical risks that may impact on this freely given consent having been addressed beforehand.

There are three privacy states in which data can be collected, analysed, used, stored, and reported. These are:

- Individually identifiable data- inttia

Identification by inference

Even when individual participants will not be named or directly identified, it is sometimes still possible for those participants to be identifiable by inference. This occurs where sufficient information about a participant will appear in the reporting of results that might enable some

indiv4892.33 (h)10.61 (e)-1 8 ()77.3 (u)25(5 (u)†)-1.2.34.3 (s1.304f-0.004 Tc 0.023 Tw -3027 0 T6.66,)Tj().02 Tc 14.81

public harm aspect, please immediately talk to the Police, for information disclosed in a survey which may indicate a less serious threat, it may be more appropriate to talk to your supervisor or line manager in the first instance.

Where and how you store and secure your data needs to be considered in your project planning.

A key consideration with regards to the location for the storage of data is the degree to which the location is secure and appropriate. For example, is it being stored on a system which is located in NZ, or another jurisdiction? Free online storage is usually unsecured and subject to other jurisdictional laws which may include the seizure or examination of your data without your consent.

The best way to ensure that you are securing your information is to store this on a University Microsoft 365 Cloud Account or the UC Server. These methods are approved by the University.

Another option is to use a properly encrypted and secured external hard drive – but remember if you do not secure this and back it up you are potentially putting the data at risk.

We do not recommend using free online providers such as Dropbox, Box, Google Docs etc. for your research. This is particularly important if you are gathering personal information and even more so if this is highly sensitive personal information.

It is important to consider who has access to the data. Some key considerations are:

- Who will have access, and in what format (e.g., will this be de-identified)?
- Will there be controls on who can access, and how they can access the data?
- Is it in a secure location, and will access to it be logged?
- What mitigations will be in place to protect the physical copies of the data? For example, how will these be secured? Who can access these “physically” (e.g., the office space)?

Acknowledgements

Thank you to both Griffith University and Otago University for the generous use of their IP in developing this document.

Griffith University – Research Ethics Manual – Privacy and Confidentiality in Human Research.

Otago University - Otago Ethics Approaches.

- why it's being collected
- who will receive it
- whether giving it is compulsory or voluntary
- what will happen if the information isn't provided.

Sometimes there may be good reasons for not letting a person know about the collection – for example, if it would undermine the purpose of the collection to protect law enforcement investigations, or it's just not possible to tell the person.

Principle 4- Manner of collection

[Principle 4](#) states that personal information must be collected in a way that is lawful and seen as fair and reasonable in the circumstances.

What is fair depends a lot on the circumstances like the individual concerned (age and capacity) and the natural sensitivity of the information. Note that threatening, coercive, or misleading behaviour when collecting information from an individual could well be considered unfair.

If you break the law when collecting information, then you have collected information unlawfully.

What is fair also depends on the circumstances, such as the purpose for collection, the degree to which the collection intrudes on privacy, and the time and place it was collected.

You need to take particular care when collecting information from children and young people. It may not be fair to collect information from children in the same manner as you would from an adult. You may need to take special care with the information of young people to address any power imbalance, and to obtain their genuine consent for the collection (or the authorisation) of their

Principle 5- Storage and security of information

[Principle 5](#) states that organisations must ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of personal information.

If an organisation has a serious privacy breach it must notify the Office of the Privacy Commissioner as soon as possible (within 72 hours).

Principle 6- Access to personal information

[Principle 6](#) states that people have a right to ask for access to their own personal information.

Principle 11- Disclosure of personal information

[Principle 11](#) means that an organisation may generally only disclose personal information for the purpose for which it was originally collected or obtained. Sometimes other reasons for disclosure are allowed, such as disclosure for a directly related purpose, or if the person in question gives their permission for the disclosure.

For instance, an organisation may disclose personal information when:

- disclosure is one of the purposes for which the organisation got the information
- the person concerned authorises the disclosure
- the information is to be used in a way that does not identify the person concerned
- disclosure is necessary to avoid endangering someone's health or safety
- disclosure is necessary to uphold or enforce the law.

Principle 12- Disclosure outside New Zealand

[Principle 12](#) sets rules around sending personal information to organisations or people outside New Zealand.

Principle 12 is a new principle in the Privacy Act 2020.

A business or organisation may only disclose personal information to another organisation outside New Zealand if they check that the receiving organisation:

- is subject to the Privacy Act because they do business in New Zealand
- will adequately protect the information, e.g. by using [model contract clauses](#), or
- is subject to privacy laws that provide comparable safeguards to the Privacy Act

If none of the above criteria apply, a business or organisation may only make a cross-border disclosure with the permission of the person concerned. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act.

Visit our [sending information overseas](#) page for more information. You can use [our decision tree](#) to

