Privacy Obligations and Considerations for Research with Human Participants

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

Introduction

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 Basics

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".

Benefits to considering Privacy

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.
- Foster an ongoing positive relationship between participants and researchers – which may aid future willingness to participate in studies.
- Protect the interests and reputations of research participants and researchers.

Statutory Privacy Considerations

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.

Responsibilities of researchers

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 without prior consent or ethical authorisation.
- Ensure that when reporting the results of the research the identity of individuals is not disclosed without their prior consent.

Privacy and recruitment

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., whānau, peers, an 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.

What student data can I use in research?

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.

Anonymity and Identification

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** - where data can be associated with individuals.
- **Re-identifiable data** - where the identifiers have been removed and replaced with a code, but it remains possible for the researchers to re-identify a specific individual.
- **Non-identifiable data** – where the data has never been labelled with individual identifiers, or from which identifiers have been permanently removed, including where it is not practicable to associate individual data with another dataset to identify individuals.

A single project may involve multiple sets of data, possibly in different privacy states (e.g., anonymous surveys, re-identifiable test results, and personally identifiable interview audio recordings). Also, during a project the privacy state of data sets may change (e.g., client files might be accessed in a personally identifiable form, they might then be analysed and stored in a re-identifiable state, and then reported without any personal identifiers).

The privacy state of the personal information will determine the approach required for consent and whether there are legislative considerations that apply.

Why is anonymity sometimes necessary?

There will be circumstances where it is preferable for participants to remain anonymous, and there are even some cases where the only ethical way to conduct the research is if the participants are anonymous. Some example considerations are:

Unequal relationship and significant concerns - where potential participants are in an unequal relationship (with the researchers or the perceived supporters/sponsors of the research) and there are significant potential concerns (e.g. there is at least a perceived risk associated with non-participation), then it might be important that no one, not even the researchers, knows who has participated in the research.

Risks - where there is at least a perceived risk associated with the collected data (e.g. disclosures of illegal behaviour), it might be preferable that no one can associate responses with individuals (e.g. in the event a law enforcement agency sought access to the data).

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 individuals to infer the identity of individual participants. This can occur with any research design, but is most commonly a factor for qualitative research where there are case study descriptions.

Example: an unnamed individual who is studying in a particular field, who is also from an ethnic minority group, and graduated high school in an identified year will be identifiable to some third parties reading the results.

The fact that identification by inference is possible does not automatically mean that the research is ethically problematic, but it does mean:

- Researchers must consider whether this identification by inference means that the research includes a degree of risk to participants or others and consider whether there is a need for research design features to manage this risk.
- The application for ethical clearance must identify this issue and discuss what, if any, steps are to be taken to address the possibility of identification and any associated risks.
- The consent and recruitment processes will need to include information about these issues so that potential participants can make an informed decision as to whether they wish to participate.

Privacy and re-use of data

It is important to consider up-front whether there will be any need for or benefit from the re-use of the information/data gathered. If there is any known intention for re-use, this should be clearly communicated to participants during the consent process.

Where the data will be completely de-identified, there are no ethical or legal privacy concerns raised by its re-use, however it is still preferrable that a full picture of future use is communicated, and that consent for this is gathered when the data is obtained. Providing the fullest picture to participants builds the strongest relationships and empowers individuals with full decision-making power.

If you are looking to incorporate or re-use information provided from another researcher, you should make the same considerations. You must ensure that you check what privacy and use statements and consents the original participants were provided with/gave. This is particularly important when drawing on information provided from outside of NZ, as the laws and requirements regarding data usage may differ.

Sharing data with other researchers

Related to the reuse of data is the sharing of data with other researchers. If the consents gathered specify the information is not to be shared, you must not share this data with another researcher.

If you are working with de-identified data which you believe you can share based on the consents gathered, you must first consider whether the data are identifiable by the researcher who will receive the data. If this is the case, it can only be shared with the consent of the participants. This is particularly of note for internal sharing of de-identified data where the data points could provide a picture of an individual to a person who knows the participants.

Even when the data is de-identified, researchers should consider whether the data is so highly sensitive that the sharing of it in anything but an aggregated form may be a concern for some participants. If this is the case, it should not be shared.

If in doubt, please consult with Chair of the Human Research Ethics Committee (human-ethics@canterbury.ac.nz), but take it back to basics – would you want this to be shared if it was about you?

Disclosure of personally identifiable information

Researchers who have access to or work with personal information should not disclose that information to other parties without the consent of the individuals named. This includes the way the results of the research are reported or published, sharing with other researchers, and reporting to third parties.

In some circumstances it may be necessary to disclose information to authorities (e.g., the Police). The Privacy Act makes provision under IPP 11 (Limits on disclosure of personal information) for certain circumstances where it is necessary to prevent or lessen a serious threat to public health and safety or the life or health of the individual concerned or another individual. If information comes to light during your research which could fall into this category, please reach out for support in how to proceed. This may depend on what the situation is - e.g., if there is a terrorism or other immediate

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.

Privacy and storage of data

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.

Access

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.

Appendix 1 – The Privacy Principles

The Privacy Act has 13 privacy principles that govern how businesses and organisations should collect, handle, and use personal information.

Principle 1 - Purpose for collection of personal information

Principle 1 states that organisations must only collect personal information if it is for a lawful purpose connected with their functions or activities, and the information is necessary for that purpose. This principle is about data minimisation.

When asking people for their personal information, think carefully about why you are collecting it. Don't collect people's identifiers such as name, phone number, etc unless it's necessary for your collection purpose. If the personal information you are asking for isn't necessary to achieve something closely linked to your organisation's activities, you shouldn't collect it.

Principle 2 - Source of personal information - collect it from the individual

Principle 2 states that personal information should be collected directly from the person it is about. The best source of information about a person is usually the person themselves. Collecting information from the person concerned means they know what is going on and have some control over their information.

It won't always be possible to collect information directly from the person concerned so organisations can collect it from other people in certain situations. For instance:

- if the person concerned authorises collection from someone else
- if the information is collected from a publicly available source
- if collecting information from the person directly is not really practicable or would undermine the purpose of collection.

Sometimes, information can be collected from other sources for law enforcement and court proceedings.

Principle 3 - Collection of information from subject - what to tell the individual

Principle 3 means that organisations should be open about why they are collecting personal information and what they will do with it. This principle is about helping people understand the reasons you are collecting their information.

When an organisation collects personal information, it must take reasonable steps to make sure that the person knows:

- 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 family/whānau.

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.

Generally, an organisation must provide access to the personal information it holds about someone if the person in question asks to see it.

People can only ask for information about themselves. The Privacy Act does not allow you to request information about another person, unless you are acting on that person's behalf and have written permission.

The rules for how an organisation must respond to a request for personal information are set out in Part 4, Subpart 1 of the Privacy Act 2020.

Principle 7 - Correction of personal information

Principle 7 states that a person has a right to ask an organisation or business to correct information about them if they think it is wrong.

If an organisation does not agree that the information needs correcting, an individual can ask that an agency attach a statement of correction to its records, and the agency should take reasonable steps to do so.

The rules for how an organisation must respond to a corrections request are set out in Part 4, Subpart 2 of the Privacy Act 2020.

Principle 8 - Accuracy of personal information

Principle 8 states that an organisation must check before using or disclosing personal information that it is accurate, up to date, complete, relevant and not misleading.

Principle 9 - Retention of personal information

Principle 9 states that an organisation should not keep personal information for longer than it is required for the purpose it may lawfully be used.

Principle 10 - Limits on use of personal information

Principle 10 means that organisations can generally only use personal information for the purpose it was collected, and there are limits using personal information for different purposes.

Sometimes other uses are allowed, such as use that is directly related to the original purpose, or if the person in question gives their permission for their information to be used in a different way.

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 help you work out if principle 12 applies to the information you are disclosing and how to comply with it.

The goal is to make sure that the privacy protections that individuals can reasonably expect under New Zealand's Privacy Act continue to apply when their information is disclosed and used in a different country.

Principle 13 - Unique identifiers

Principle 13 sets restrictions on assigning identifying numbers and other unique identifiers to individuals. The principle states that an organisation can only assign unique identifiers to people when it is necessary for its functions.

Unique identifiers are individual numbers, references, or other forms of identification allocated to people by organisations as a way to uniquely identify the person to the organisation assigning the identifier. Examples include driver's licence numbers, passport numbers, IRD numbers, or National Health Index (NHI) numbers.

An organisation cannot assign a unique identifier to a person if that unique identifier has already been given to that person by another organisation. For example, this prevents the Government from giving you one personal number to use in all your dealings with government agencies.

However, an organisation can record (and use) a person's unique identifier so that they can communicate with another organisation about the individual.

Organisations must also take reasonable steps to protect unique identifiers from misuse and make sure they verify someone's identity before assigning a unique identifier.