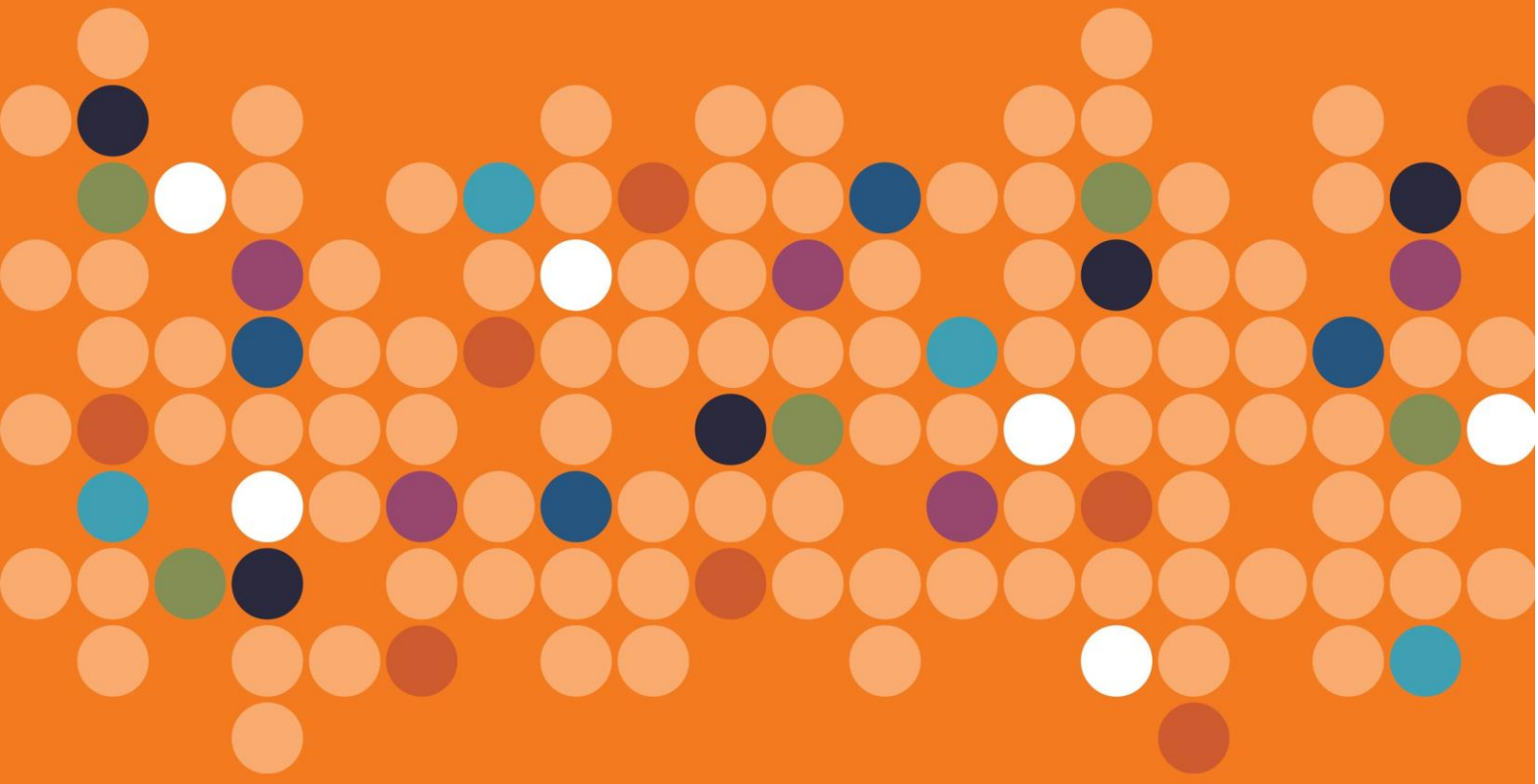
January 2022 | Version 1.2

Data Protection & Use Policy (DPUP)

Respectful • Trusted • Transparent



SOCIAL WELLBEING AGENCY | TOI HAU TĀNGATA

Policy developed in collaboration with the social sector

New Zealand Government

Te Tari Taiwhenua Internal Affairs

Document Control

Version	Date	Author	Description
1.1	20 Sep 2020	DM	Published late 2020 to include updates made in Privacy Act 2020.
1.2	06 Dec 2021	DM	Updating passages following content re-design for digital.govt.nz/dpup.

NOTE: This is the updated master version of the Data Protection and Use Policy, captured from the original master PDF file on the dpup.swa.govt.nz website, and saved as a Word document. The document control section above captures the change history. Some visual elements of the original file are retained purely because of the transformation from a designed PDF file to an editable MS-word file. However, in terms of visual presentation of the content in this file, the master version of that is now part of privacy, at www.digital.govt.nz/dpup.

Not legal advice

The Social Wellbeing Agency has taken all due care in preparing this guidance. Please note, however, that it is not legal or other advice. You are responsible for taking whatever advice you may need in a particular situation.

Citation

Social Wellbeing Agency 2021.

The Data Protection and Use Policy. A Policy for the respectful, trusted and transparent use of people's data and information in the social sector.

The Policy is based on engagement findings from the 'Your voice, your data, your say' engagement on social wellbeing and the protection and use of data.

ISBN 978-0-473-55251-0

Introduction

What the Data Protection and Use Policy (DPUP) is

The Data Protection and Use Policy (DPUP) describes what 'doing the right thing' looks like when you collect or use people's personal information.

DPUP is for all New Zealanders, particularly agencies and the people who use their services.

DPUP uses the term 'agency' to refer to government agencies, non-governmental organisations and other providers of services.

Read the 1-page DPUP overview:

Data Protection and Use Policy — an overview
Data Protection and Use Policy — an overview (PDF 127KB)
Data Protection and Use Policy — an overview (PPTX 1.2MB)

DPUP's key concepts

DPUP puts people first. It's about respectful, trusted and transparent use of people's personal information.

DPUP provides good-practice advice about collecting and using people's information. It recommends practices that in some places go beyond the law, and in those situations says clearly why it does so. This is because when information is no longer 'personal' in terms of the law, it may remain deeply personal and sensitive to the communities it comes from, describes, or is about.

DPUP supports agencies to:

- be clear about the vital importance of purpose when collecting and using people's personal information
- help people to understand what's happening with their information and what choices they have
- make it easy for people to see and request correction of their information
- work together for better insights and outcomes.

Although DPUP is not mandatory, agencies are encouraged to adopt it in a way that makes the most sense for their agency, their work and their communities.

Cabinet endorsed DPUP in November 2019.

The Data Protection and Use Policy — Social Wellbeing Agency

Introduction to DPUP

This 3.5-minute video explains DPUP's key concepts, who it is for, and how it was developed.

DPUP Introductory Video

Personal and non-personal information

DPUP uses the terms 'personal information' and 'non-personal information'.

- Personal information is information that does, or could be used to, identify individual people.
- Non-personal information does not identify individual people, and cannot be used to, even if it is combined with other information.

DPUP states when its advice applies to personal information, non-personal information, or both. It also uses the terms 'data' and 'information' interchangeably.

DPUP terminology
Making personal information safe for reuse

DPUP's structure

DPUP consists of 5 Principles and 4 Guidelines. These make up the policy. It also includes practical guidance that wraps around the policy, so agencies can use it in their work.

The Principles focus on values and behaviours. The Guidelines bring the Principles to life by explaining good practice in critical areas that make the most difference. This has a significant impact on people's trust and confidence.

Although the Principles and Guidelines are different, they overlap, and this is intentional.

DPUP Principles

These define a common set of values and behaviours. They help agencies to provide people with respectful and transparent interactions and practices.

Because the Principles have people and their wellbeing at the centre, the focus for agencies is on relationships, rather than rules. It's a way of working that respects people, their information and their stories.

The Principles were developed to respect and acknowledge cultural considerations. A range of Māori stakeholders contributed to the Principles, and their names and meanings.

The 5 Principles are:

He Tāngata

- Focus on improving people's lives — individuals, children and young people, whānau, iwi and communities.
- Strive to create positive outcomes from any collection, sharing or use of data and information.
- Use checks and balances and ensure that the information collected or used is reasonably necessary for the purpose.

He Tāngata Principle

Manaakitanga

- Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information.
- Recognise and incorporate diverse cultural interests, perspectives and needs.
- Include and involve service users whenever possible.
- Incorporate people's views when they have a specific interest in what is done with their information.

Manaakitanga Principle

Mana Whakahaere

- Empower people by giving them choices and enabling their access to and use of their data and information.
- Where possible, give people choices and respect the choices they make.
- Give people easy access to and oversight of their information wherever possible.

Mana Whakahaere Principle

Kaitiakitanga

- Act as a steward in a way that people understand and trust.
- Recognise you are a kaitiaki rather than an owner of people's information.
- Be open and transparent — support people's interest or need to understand.
- Keep data and information safe and secure and respect its value.
- If there's a privacy breach, act quickly and openly.

Kaitiakitanga Principle

Mahitahitanga

- Work as equals to create and share valuable knowledge.
- Work with other agencies to create and share value together.

- Carefully share relevant information so people get the support they want and need.
- Grow collective knowledge and improve services through 2-way sharing of non-personal information.

Mahitahitanga Principle

DPUP Guidelines

These key activities describe good practice and ways to apply the Principles to an agency's everyday business. The Guidelines help agencies to understand and apply good practice, including many key aspects of the Privacy Act 2020, in relation to these activities.

Agencies need to apply the Guidelines in a way that makes sense for the:

- type of work they do
- people they work for
- range and sensitivity of information they hold about people.

The 4 Guidelines include:

Purpose Matters

- Be clear about the purpose of collecting or using people's information. Collect only what is needed.
- Consider how using people's information might affect their wellbeing and their trust in those using it.

Purpose Matters Guideline

Transparency and Choice

- Be transparent and help people understand why their information is needed and what happens with it.
- As much as possible, support their choices about what they want to share and how they want it used.

Transparency and Choice Guideline

Access to Information

- Be proactive about supporting people to understand what information is held about them, their rights to access it and ask for corrections to be made.
- Look for ways to make this easy and safe for service users.

Access to Information Guideline

Sharing Value

- Work together to ensure information used to create insights is relevant and usefully describes real experiences.
- Share insights to help grow knowledge and support wellbeing.

Sharing Value Guideline

Practical guidance

The practical guidance under 'Before you start to use DPUP' and 'Use DPUP in your work' includes information, examples and resources to support you in applying DPUP in your everyday work.

The guidance helps you to:

- develop a good understanding of DPUP
- plan for adopting DPUP in your organisation
- apply DPUP in your work.

Before you start to use DPUP

Use DPUP in your work

Who DPUP is for

The Data Protection and Use Policy's (DPUP's) focus on respect, trust and transparency leads to better quality services that can benefit all New Zealanders.

Using DPUP benefits agencies and people

When an agency adopts DPUP, the people who use the agency's services benefit by:

- knowing what they can expect from the agency
- knowing their information will be treated respectfully
- understanding and trusting why and how their information might be used
- being better placed to act on their rights to access and request changes to their information.

All agencies benefit from adopting DPUP by:

- developing a richer understanding of their obligations to the people who use their services
- supporting transparent and ethical use of data.

Public sector agencies benefit from adopting DPUP by:

- increasing public trust and confidence
- increasing their maturity level as measured by the Government Chief Privacy Officer's (GCPO's) Privacy and Maturity Assessment Framework
- aligning with the Public Service Code of Conduct.

Gaining buy-in for a privacy programme
Public Service Code of Conduct — Public Service Commission

Creating a trust cycle

Agencies that collect, share and use information in a respectful and transparent manner create a cycle of trust between themselves and the people who use their services. By better understanding when and how people's information might be used, agencies can:

- increase the accuracy, relevance and value of people's information to communities
- build trust that the agency values respectful and transparent use of people's information.

Using DPUP benefits specific roles

Ensuring good practice when collecting and using people's information is not just for privacy officers, it's a collective responsibility.

DPUP was developed for government agencies, non-governmental agencies and other service providers that collect people's information, use it in their work, or define or design new services or contracts that rely on it to enhance people's wellbeing.

It's good practice to use DPUP if you:

- work in the front line — for example, case managers, call centre operators
- manage or lead frontline workers — for example, team leaders, people leaders
- work in funding, contracting and partnering — for example, business advisors, relationship managers
- develop policies, services and programmes — for example, solution architects, policy analysts, service designers
- work in analysis, research and evaluation — for example, data scientists, business analysts.

Use DPUP in your work
Agency responsibility

What role leadership plays

An agency's leadership also has a crucial role in building and maintaining public trust. This depends in part on ensuring that people know their personal information is used in a respectful, transparent and trusted way.

Leadership's role is to focus on the connection between a people-centred approach to privacy, and the positive effect on public trust and service quality.

If leadership champions the views of the people and communities they serve, this enables the teams working with people's information to understand and to do the right thing when collecting or using it.

The GCPO has provided agencies with core expectations about good practice for privacy management and governance. This also describes the leadership contribution, the critical importance of collective responsibility, and other features of good privacy maturity.

Core expectations

Why DPUP was developed

The Data Protection and Use Policy (DPUP) was developed by the Social Wellbeing Agency to provide a shared set of rules for the respectful, trusted and transparent use of personal information.

Developing DPUP

DPUP was developed to provide both government agencies and non-governmental organisations (NGOs) with clear guidance about what's reasonable, and what's not, when collecting or using people's personal information. Creating and maintaining authentic relationships, and trust, with different communities is important.

Developing DPUP involved broad engagement with a diverse range of people from a variety of agencies and communities. The engagement aimed to understand their view of what agencies need to do to:

- establish and maintain respectful use of people's information
- build trust and confidence between people and agencies.

DPUP's Principles and Guidelines were created from their thoughts, ideas, experiences and viewpoints.

Data Protection and Use Policy — Social Wellbeing Agency

Refining the Principles and Guidelines

The engagement produced many ideas and suggestions about what the policy required. Once refined, these became DPUP's 5 Principles and 4 Guidelines. The Principles are the values and behaviours behind collecting and using personal information that should be part of an agency's culture. The Guidelines are the key topics and processes that will help agencies put the Principles in place.

The He tāngata Principle sprang from the community design sessions and has a special role. It wraps around DPUP as a whole. It is a reminder that everything an agency does with personal information should be with the following question in mind: "How does this contribute toward the wellbeing of the individual, or community?".

To learn more about the engagement results, 'What you told us' and 'From Listening to Learning' on the Social Wellbeing Agency website provides more detailed information.

What you told us — Social Wellbeing Agency
From listening to learning — Social Wellbeing Agency (PDF 476KB)
Read the DPUP Principles
Read the DPUP Guidelines

Revising the Privacy Maturity Assessment Framework

In 2021, the Government Chief Privacy Officer revised the Privacy Maturity Assessment Framework (PMAF). This revision put a greater focus on the:

- people who provide information to agencies
- diverse responsibilities that contribute to good privacy maturity
- relationship between good privacy practice, good service delivery and agencies' duty to build and maintain public trust.

DPUP fits well with this shift.

Privacy Maturity Assessment Framework (PMAF) and self-assessments

Working with other laws and guidance

DPUP provides good-practice advice about the collection and use of people's information. In some areas, and for good reasons, that advice goes beyond the law.

DPUP's relationship to other laws and guidance.

How the DPUP Guidelines and Principles support each other

While the Data Protection and Use Policy (DPUP) Principles describe values and behaviours, the Guidelines offer detailed advice on key topics that are relevant to different situations and roles.

You can read about when to use the guidelines, and how they support each other, here:

How the DPUP Guidelines and Principles support each other.

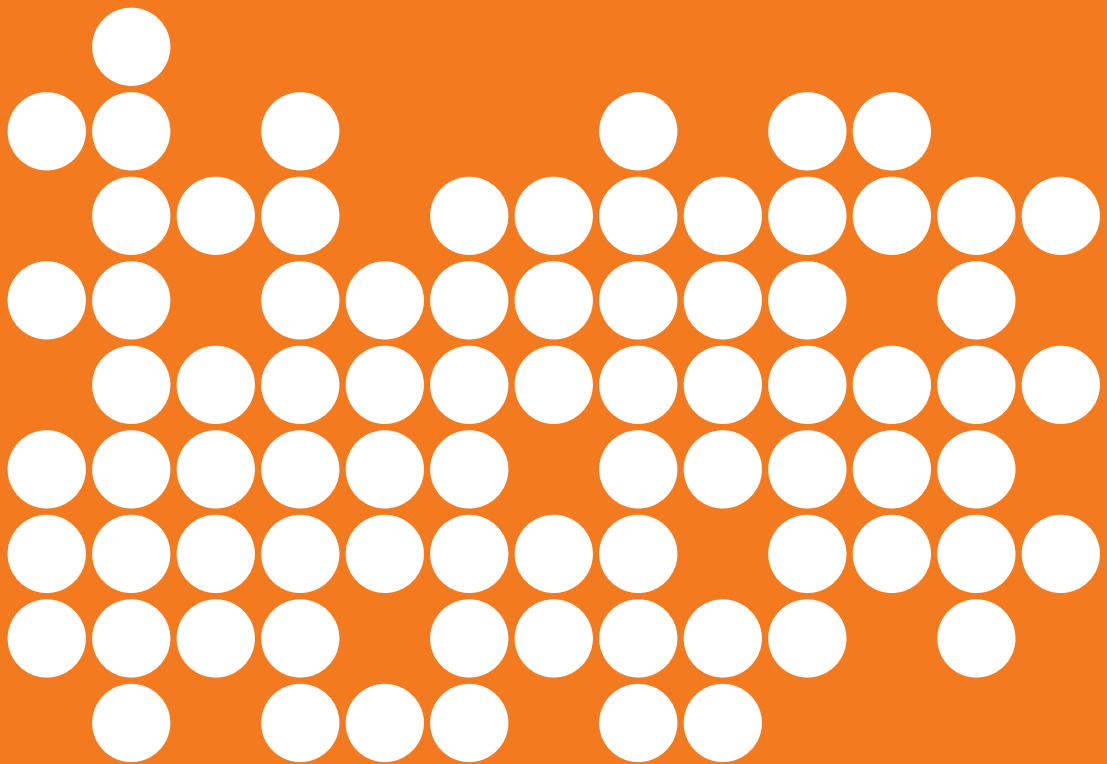
Using DPUP in your work

DPUP provides practical good practice guidance on what "doing the right thing" looks like. A range of resource for working with DPUP in the context of typical roles and activities can be found on digital.govt.nz.

Using DPUP in your work

Policy Principles

The 5 Principles in the Data Protection and Use Policy (DPUP) focus on people and wellbeing to help agencies provide respectful, trusted and transparent interactions and practices.



DPUP Principles

Overview of Principles

The 5 Principles in the Data Protection and Use Policy (DPUP) focus on people and wellbeing to help agencies provide respectful, trusted and transparent interactions and practices.

The 5 Principles articulate values and behaviours:

- to help ensure data practices are focused on the wellbeing of people and communities
- that underpin the respectful, trusted and transparent use of data
- that work together and reinforce each other.

He tāngata

Focus on improving people's lives — individuals, children and young people, whānau, iwi and communities.

The He Tāngata Principle has a special role. It wraps around DPUP as a whole. It reminds us that everything we do with data should be with this question in mind: "How does this contribute toward the wellbeing of the individual or community?

Manaakitanga

Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information

Mana whakahaere

Empower people by giving them choice and enabling their access to, and use of, their data and information

Kaitiakitanga

Act as a steward in a way people understand and trust

Mahitahitanga

Work as equals to create and share valuable knowledge.

Development of the Principles

DPUP's engagement and design processes were developed to ensure the final policy genuinely incorporates the voices of many people and agencies.

As DPUP developed, it became clear that the Principles, Guidelines and related behaviours aligned with te ao Māori values. During the engagement and design process, and in collaboration with the Social Wellbeing Agency's Chief Māori Advisor, conversations were held with various individuals and groups to determine how the Principles fitted with te ao Māori values and how each Principle could be best described in te reo Māori.

Māori words, or kupu, are rich in meaning and can mean many things. Read the Principles in detail to find the meaning of the kupu chosen to describe each Principle in the context of the DPUP. These kupu have been tested with a range of Māori stakeholders.

He tāngata

The use of *he tāngata* comes from the whakataukī (Māori proverb)

> ***"he aha te mea nui? Māku e kii atu, he tāngata, he tāngata, he tāngata"***

which translates to:

> ***"What is the most important thing in the world? Well, let me tell you, it is people, it is people, it is people"***

So, in this context, the use of he tāngata means that people — individuals, whānau and communities — are placed at the centre of everything we do.

The goal of lifting them up, empowering them and improving their wellbeing is at the forefront of how we care for them and their information. It reminds us that when working with people's information, we are working in their service.

Manaakitanga

Manaakitanga means the process of showing respect, generosity and care for the people who use services, their whānau and communities. It also means to show respect and care for their information and stories.

Mana is the essential lifeforce within a person, place or object. In this context, caring for the people who share their information involves supporting, listening to and involving people in deciding what happens to their information. This results in empowering people and enhancing their mana.

Mana whakahaere

Mana whakahaere means governance, authority, jurisdiction, management, mandate and power. Mana in the context of the Data Protection and Use Policy (DPUP) refers to an individual's power or influence, and whakahaere refers to an individual's ability to influence or manage.

To say that an individual has mana whakahaere over their data recognises the importance of their choice or say over where their data will go, who can access it and what it can be used for.

Kaitiakitanga

Kaitiakitanga means to have guardianship and stewardship of people's data and information. This is a trusted role that protects and keeps people's stories and information safe, respects what has been shared, understands its value and enables the sharing of that information when that is appropriate.

The kaitiaki or guardian realises that they do not own this information but keep it in trust — making it easily accessible for the person whose information it is and growing the value of the information. Growth can mean using the information to create and share insights, or returning collective, non-personal data back to the people and community it came from for their use.

This type of stewardship results in benefits and wellbeing for the individual, whānau and wider communities both now and between generations — protecting information and delivering value into the future.

Mahitahitanga

Mahitahitanga expresses partnership, collaboration and cooperation. It refers to effectively engaging with one another and working together as equals in day to day activities.

There is recognition that the value of the mahi is enhanced when everyone contributes their knowledge, experience and wisdom. It is a commitment to one another and the process.

When people are supported and cared for throughout the mahi, this provides and inspires valuable knowledge and insights that benefit everyone.

He tāngata

Focus on improving people's lives — individuals, children and young people, whānau, iwi and communities.

The He Tāngata Principle has a special role. It wraps around the Data Protection and Use Policy (DPUP) as a whole. It reminds us that everything we do with data should be with the following question in mind.

"How does this contribute toward the wellbeing of the individual or community?"

Strive to create positive outcomes from any collection, sharing or use of data and information

- Any collection, use or sharing of data and information must be for a reasonable and well-defined purpose.
- There should be an easy to understand, tangible link between the purpose for which data or information is collected, used or shared, and the benefits for people. The benefit might be for certain individuals, whānau, a community or iwi, or the benefit may be a public good.
- Because actions and outcomes are not always clear cut, risks and potential negative outcomes should be assessed so it's clear how these balance against positive outcomes.

Use checks and balances and ensure that information is reasonably necessary for the purpose

- Data and information exist in many different forms. Some information is more suitable or acceptable for certain purposes than others. Look at the purpose carefully before considering what information makes the most sense to use.
- Some purposes need more oversight and checks than others to make sure they are well-defined and reasonable.
- Only the minimum information needed to achieve the outcome should be collected, used or shared

Manaakitanga

Respect and uphold the mana and dignity of the people, whānau, communities or groups who share their data and information.

Recognise and incorporate diverse cultural interests, perspectives and needs

- Be mindful of New Zealand's cultural diversity, and the different perspectives, needs and approaches that should influence how we work.
- Consider the views of people and communities. Learn what they think about why and how their data and information is collected, used or shared.
- When deciding what information to collect and use to develop insights, recognise that different groups and people may value qualitative and quantitative information about themselves differently.
- Advocate for having a diverse, informed and representative membership for data and information advisory groups, reference groups and other kinds of groups to ensure quality practice and outcomes.

Include and involve service users whenever possible

- People can offer greater value than just their information and data.
- Their ideas and views are valuable. Include these when developing or testing proposals to collect and use data or information to improve wellbeing.

Incorporate people's views when they have a specific interest in what is done with their information

- For Māori, this means upholding their rights as Treaty partners and focusing on the collective and whānau outcomes of any work.
- For Pacific peoples, this means considering the distinct views and thoughts of their diverse communities.
- For children and young people, this means supporting their right to participate, communicating with them in appropriate ways and at the appropriate level, and acknowledging what they have to say is valuable.
- For disabled people, this means considering accessibility issues, focusing on what works well for them, understanding their achievements and contributions, and making sure they are not 'invisible' in data and information.
- Other people and groups are likely to have their own specific needs and priorities. It is important to be proactive in identifying and addressing those needs and priorities.
- Employing people with the relevant cultural competence and experiences will help service delivery agencies engage effectively with these communities and groups.

Mana whakahaere

Empower people by giving them choice and enabling their access to and use of their data and information.

Where possible, give people choices and respect the choices they make

- Tell people, in a way that makes sense to them, what data or information is collected about them, how it's used, who it's shared with, and why, even if it's used or shared in a way that does not and cannot be used to identify them. There will be situations where there are good reasons not to tell them, for example, if it would undermine the purpose of the collection, or it's just not possible to tell the person.
- Consider people's wellbeing and provide choices about what is collected, how it's used and why, and whether it's shared — unless it's not safe or appropriate to do so.
- Take extra care when deciding not to give people choices or not to explain to them how their information will be used and why.
- It's not appropriate to rely on broad or 'future-proofing' purpose statements or consents for potential uses that are loosely defined.
  Even when there is no legal requirement to tell people, transparency is important for trust and respect, and recognising people's mana.
- If it's not timely or appropriate to tell them beforehand, tell them afterwards — unless there's good reason not to.
- When communicating with children and young people, consider their vulnerability and the roles that their parents, guardians or wider whānau may play in supporting them.

Give people easy access to and oversight of their information wherever possible

- People should not have to rely on Privacy Act 2020 requests to access information held about them.
- Encourage people to see what is recorded about them. This is a way to empower them and acknowledge that their data and information is part of their story and experiences.
- Making it easy for people to see their data and information can mean many things. This may include showing them what is written on a computer screen, including them on email referrals to another agency (taking care to double-check email addresses), or providing information in accessible formats for people with a sight disability or limited literacy.
- Whenever possible, help people check, add or correct their information.
- Help people access their information so that they can share it with others and avoid retelling their story.

Kaitiakitanga

Act as a steward in a way that people understand and trust.

Be a kaitiaki rather than an owner of people's information

- Those who collect, use, share and store data and information are kaitiaki, stewards and caretakers, not owners, of that data and information.
- Being a kaitiaki is about working in the service of, and being accountable to, New Zealanders around the collection, use and sharing of their data and information, and ensuring that it is valued and respected.
- A kaitiaki recognises the importance of people being able to access their information and helps them do that.

Be open and transparent — support people's interest or need to understand

- Have open conversations about the collection, use and sharing of data and information and the reasons for them. This means building trust, being inclusive, respecting a wide range of views, and working in partnership.
- Explain things in an accessible and easy to understand way, and in a manner that matches people's needs and interests. Use different types or formats of data and information, as well as levels of detail, to match different interests, levels of comprehension, context and needs of different groups.

Keep data and information safe and secure and respect its value

- Use data management practices that are safe and secure. Keep in mind the nature of the information and data, as well as how it is being collected, used, shared, analysed and reported.
- Those who collect data and information need easy-to-use tools and processes for accurately and efficiently collecting, using and sharing information.
- Treat data as a valuable asset. Store and maintain it so that it is accessible and reliable, and only keep it for as long as it is necessary and relevant.
- Those who hold people's information are able to grow its value. They may do this by creating and sharing insights, or by returning collective, non-personal data back to the people and community it came from for their use. In all cases they must comply with the law, protect people's privacy and maintain people's trust and confidence.

Mahitahitanga

Work as equals to create and share valuable knowledge.

Work with other agencies to create and share value together

- Consider other agencies' resource needs and costs if your agency relies on them to collect, store or use data, including applying good information practices.
- Include a wide range of people in projects or activities that collect or use people's information so capacity and knowledge grow. Other agencies may have an interest in using that information to improve wellbeing, and may contribute to exploring new ideas.
- Work with others who collect data and information to minimise duplication, as well as the burden on people who gather or share information.
- Work with iwi and other Māori groups as Treaty partners regarding personal data and information. Involve them in decisions over data and information issues that affect them.

Carefully share information so people get the support they want and need

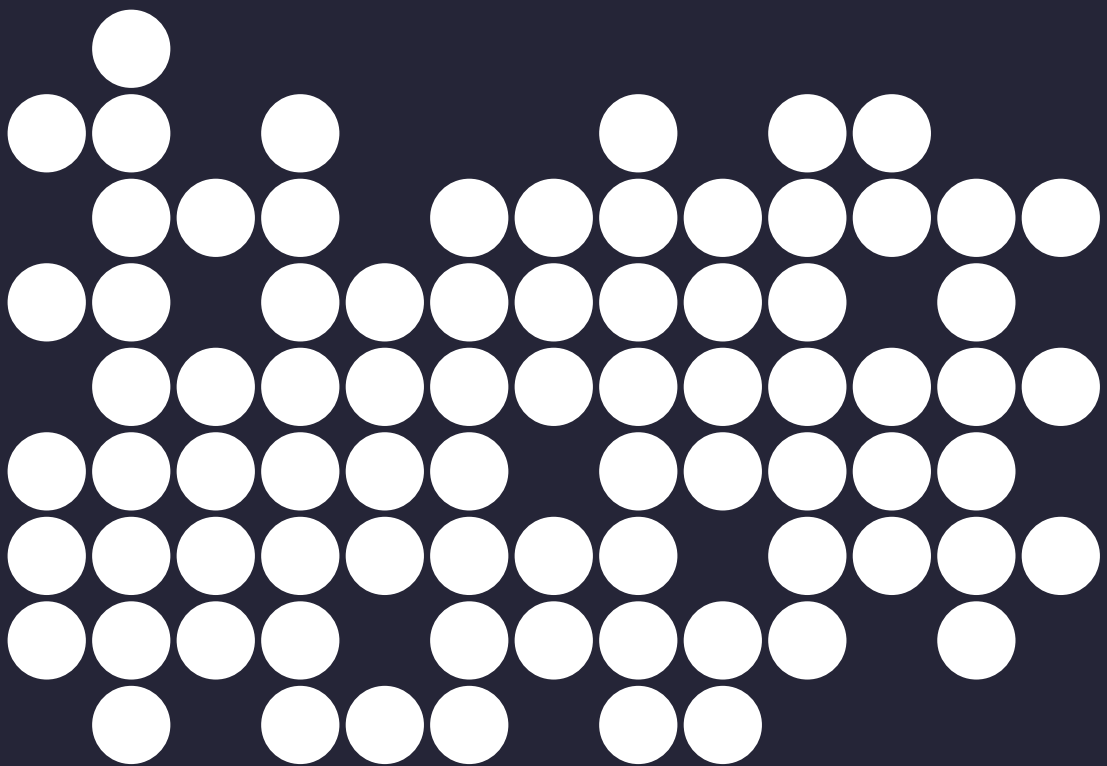
- Enable other professionals to support people by making sure they have the information they need to do their work, within what the law permits.
- Recognise the diverse and complex nature of the services government offers and use it as an opportunity to connect with others to improve outcomes for individuals. In many situations, no single professional or agency will have the whole picture.

Grow collective knowledge and improve services through 2-way sharing of non-personal information

- People's non-personal information such as de-identified data, analysis, results and research findings can often be useful to others working with relevant communities.
- Enable organisations or groups with a clear and legitimate interest to safely and easily access and use government-held data sets in a de-identified form for locally led development.
- Share expertise and help others understand and use data accurately and safely, for example, ensuring that people are not re-identified.
- Advocate for, and support 'by / for' research (like Kaupapa Māori) so communities or groups better understand their own goals and priorities and the needs of their people.
- Create feedback loops with people and organisations who contribute data and information. Tell them the outcomes of any use of their data and the value it created.

Policy Guidelines

The Data Protection and Use Policy (DPUP) Guidelines describe key activities and processes to help put the Principles in place.



DPUP Guidelines

Overview of the Guidelines

The Data Protection and Use Policy (DPUP) Guidelines describe key activities and processes to help put the Principles in place. The Guidelines also help agencies to understand and apply the Privacy Act in relation to these key activities.

The key activities covered by the Guidelines were identified during engagement as those that make the greatest contribution to respect, trust and transparency.

You can read the 4 Guidelines in any order, but **Purpose Matters** has a central role. It responds to a key theme from the engagement phase summarised by: "It all starts with why". Understanding this topic has implications for the other Guidelines.

Purpose Matters is about:

- the importance of being clear about the 'why' when thinking about collecting or using people's information
- only collecting what is needed
- how collection or use of people's information could affect their wellbeing

Watch a 90-second video that explains the key concepts of this Guideline: https://youtu.be/63YGXOS8MQ4

Transparency and Choice is about enabling people to understand:

- what is happening with their information
- what choices they have
- helping them understand the 'why'
- what rights they have to access and request changes

Watch a 90-second video that explains the key concepts of this Guideline: https://youtu.be/DBK0tWRFnZY

Access to Information is about:

Making it easy for people to see and request correction of their information.

Watch a 90-second video that explains the key concepts of this Guideline: https://youtu.be/ozXtRw0mq0Y

Sharing Value is about:

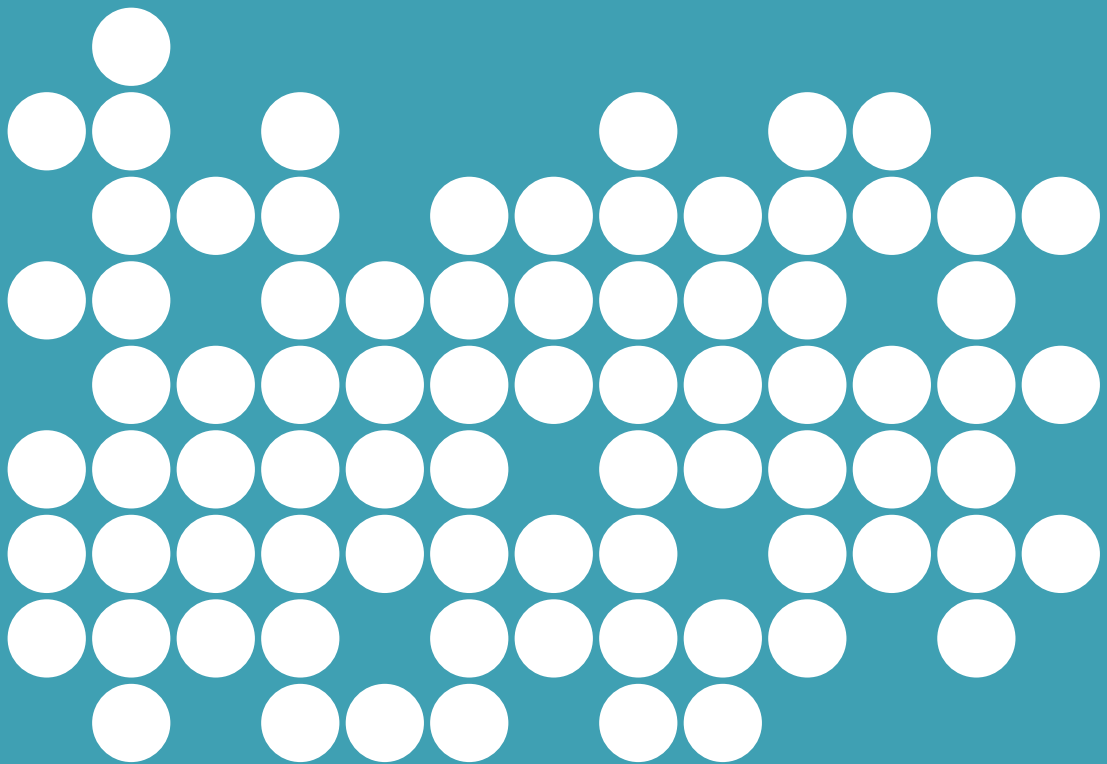
- working together for better insights and outcomes
- the importance of being inclusive to ensure that information used to create insights is relevant and usefully describes real experiences
- sharing insights that deliver value and improved wellbeing

Watch a 90-second video that explains the key concepts of this Guideline: https://youtu.be/auwpsJAYWkc

Guideline

Purpose Matters

The vital importance of purpose to collecting and using people's information.



Purpose Matters Guideline

Why DPUP has a Purpose Matters Guideline

Purpose Matters' intent

This Guideline helps agencies who are considering collecting and using people's personal information clarify why they are collecting that information.

The first part of this Guideline explains important aspects of legislation (particularly the Privacy Act 2020) that are relevant to:

- purpose and collection of personal information
- purpose and use of personal information
- purpose and sharing of personal information.

This Guideline then describes an approach to defining and assessing proposed purposes. The approach focuses on:

- being clear about how the personal information contributes to the outcomes to be achieved
- being clear about the method that will be used to achieve the outcomes
- considering the context in which the information is being collected and used.

It also provides a range of checks and balances that can help determine if:

- a proposed collection or use is lawful and appropriate
- there's a need to get input from others, and when to seek it.

Purpose Matters' key concepts

Agencies must be clear about why they collect personal information as it informs many of the key decisions made with people's information.

- Agencies can only collect personal information for lawful purposes connected with their functions or activities.
- Agencies can only collect personal information to the extent reasonably necessary for those lawful purposes, or as otherwise permitted by specific statutory provisions.
- Agencies should, when considering what's reasonably necessary, look at the intended outcomes together with their processing methods and the context of use.
- In some cases, the context may suggest that, even where a purpose of collection is lawful and it's reasonably necessary to collect personal information for that purpose, proceeding with the collection may be ethically questionable or otherwise undesirable.
- Agencies can only use personal information for the purposes it was collected for, unless it can legally be used or disclosed for other purposes.

Addressing concerns

Before and during the Data Protection and Use Policy's (DPUP's) engagement stage, non-governmental organisations (NGOs), people who use agencies' services, and the Office of the Privacy Commissioner expressed concerns that directly relate to the purpose of collecting people's information.

Those concerns included:

- if agencies are not clear enough about why they collect personal information and how they inform people of that purpose, then:
    - agencies might collect more information than they need, which is unlawful and inappropriate

    - agencies that collect personal information from other agencies (who collect it directly from people) are not able to tell those other agencies what they need to know, and this can put those other agencies in a difficult position as they may not know if they should provide the information or what to tell the people they collect it from
- agencies give enough thought to how appropriate it is to collect, use or share certain kinds of personal information, even when the law allows it.

Ensuring information collection is legal and ethical

This is one of DPUP's most important Guidelines. This is because it's important that agencies:

- approach questions of purpose with enough precision.
- understand that purpose informs many important decisions with people's information

This helps them to approach information collection in a manner that is legally and ethically sound. Not doing this may result in:

- legal problems with otherwise sound policy or service initiatives
- failure to deliver intended wellbeing outcomes for people
- a loss of trust and confidence from the people that agencies serve

Important reasons for this Guideline

- Service providers, including government agencies, NGOs and other providers, view the respectful, trusted and transparent use of people's personal information as a joint responsibility for collective benefit. A lack of understanding or clarity about the purposes of collection, use or sharing can undermine that responsibility.
- NGOs often say that better clarity on the purpose of collecting and using information is the topic of greatest importance to them.
- People who use services understand that agencies may want to use their information to improve outcomes for people in similar situations. However, they still want clarity on the purpose for collecting and using their information. For example, agencies telling people they need their information for research purposes is not helpful.
- Understanding purpose and getting it right can help an agency earn people's trust and confidence. This is vital to ensure what it's doing is both lawful and ethically justifiable.

Be clear about purpose and collection

The Data Protection and Use Policy (DPUP) helps agencies understand the importance of purpose and what's appropriate when they consider collecting people's personal information.

Before collecting personal information

Agencies must be clear about the purpose they are collecting the personal information for.

- Under the Privacy Act 2020's information privacy principle 1 (IPP1) — Purpose of collection of personal information, agencies should not collect personal information unless it is for a lawful purpose connected with their functions or activities and, importantly, the collection is reasonably necessary for that purpose.
- If agencies are collecting personal information under a specific statutory power that authorises or requires the collection, they need to be clear on the purpose of collection to ensure the statutory power covers the information they propose to collect and the reason for collecting it.

IPP1: Purpose for collection of personal information — Office of the Privacy Commissioner

> Purpose will **always** be relevant. It's important to assess and articulate it properly for both legal compliance and to guard against indiscriminate or excessive collection of people's information.

Collecting information from people or other agencies

Clarity of purpose is vital regardless of whether agencies are collecting information directly from people or from other agencies and organisations. The reasons for that go beyond ensuring that a collection is lawful under either IPP1 or a specific statutory collection power.

- If agencies are collecting information from people, clarity of purpose is vital to helping people understand why their information is being collected, as is usually required by the Privacy Act 2020's IPP3 — Collection of information from subject. As the Office of the Privacy Commissioner has observed that, "it is fundamental to people's right to privacy that, when providing information about themselves, individuals know why the information is being collected and what it is going to be used for". This topic is discussed further in the Transparency and Choice Guideline.
- Sometimes providing people with details about the collection of their information, who will receive it, the reasons for doing so and other matters listed in IPP3 could undermine an agency's reason for collection and could therefore justify not telling them. However, the relevant exception in IPP3 that would justify not telling them applies where doing so would "prejudice the purposes of the collection". If the purposes of collection have not been clearly articulated, it will be difficult to rely on this exception. Without clarity of purpose, it may also be difficult to rely on other exceptions in IPP3.
- Information needs to be collected from the relevant individuals unless an agency is authorised or required by a specific statutory provision to collect personal information from another agency or an exception in the Privacy Act 2020's IPP2 — Source of personal information applies. One of those exceptions is that collection directly from the individuals concerned would "prejudice the purposes of the collection". Again, if the purposes of collection have not been clearly articulated, it will be difficult to rely on this exception. And again, without clarity of purpose, it may also be difficult to rely on other exceptions in IPP2.

IPP2: Source of personal information — Office of the Privacy Commissioner

IPP3: Collection of information from subject — Office of the Privacy Commissioner

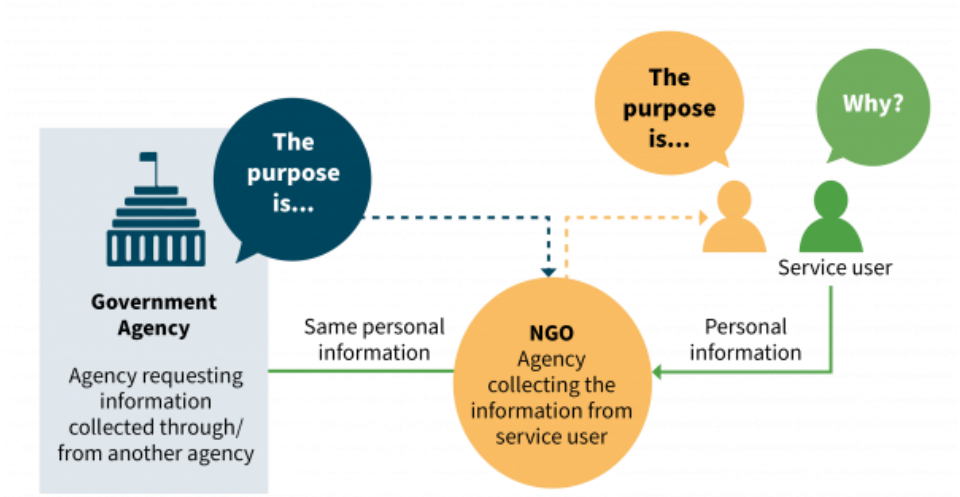
When other agencies need to understand the purpose of collection

This is an example of a government agency collecting personal information from a non-governmental organisation (NGO) that collects it directly from people. However, the guidance can be applied to any agency collecting information from another.

If a government agency collects personal information from an NGO, it's important the government agency:

- has a clearly articulated and lawful purpose of collecting the information from the NGO
- fully informs the NGO of the government agency's purpose of collection in a manner that is easy for the NGO to understand and explain to its service users
- tells the NGO about the government agency's purpose, so the NGO can include that in its statement of purposes to the people it serves.

Diagram 1: Government agency collecting information from an NGO



Detailed description of the diagram.

The diagram shows that a government agency collecting information from another agency (an NGO) about their service users, needs to tell the NGO what they are going to do with the information.

The diagram shows an image of the beehive representing a government agency and the words underneath: "Agency requesting information collected through / from another agency."

A dotted arrow comes out of a speech bubble from the beehive saying "The purpose is…" and goes to a circle that represents the NGO / agency collecting information from the service user.

A dotted arrow, representing the purpose for collection, goes from the NGO circle to 2 service users / people icons who are asking "The purpose is…" and "Why?"

A solid arrow representing their personal information goes from them to the NGO. A solid arrow representing that same personal information goes from the NGO to the beehive / government agency.

The government agency should also tell the NGO if providing the agency with the information for the specified purposes is voluntary or mandatory. If mandatory, then the government agency needs to say what particular statutory provision this is under.

The Privacy Act 2020 does not specify all of these requirements, in terms of what the government agency needs to tell the NGO, but they are often vital. If the NGO does not fully understand these collection requirements, it could struggle to assess:

- if it is lawful to provide the information to the government agency
- if it must or only may provide the information to the government agency
- where providing the information is voluntary, if it should provide the information to the government agency.

In addition, it might not be able to meet its own transparency obligations to service users under IPP3.

The NGO will value the government agency providing this information proactively. If the NGO wishes to ask further questions, it's important the government agency respects the NGO's right to make the request and provides the information in a responsive and respectful manner to ensure the NGO knows it is welcome to ask such questions whenever it needs to.

If identifying information is not required, do not ask for it

IPP1 says do not collect personal information unless it's reasonably necessary for a lawful purpose connected with an agency's functions or activities. If a collecting agency can achieve its purpose without collecting identifying information (personal identifiers such as name and residential address), then it should not collect it.

The Privacy Act 2020 makes this clear with its new IPP1(2): "If the lawful purpose for which personal information about an individual is collected does not require the collection of an individual's identifying information, the agency may not require the individual's identifying information."

Part 3 of the Privacy Act 2020: Information privacy principles — Parliamentary Counsel Office

Be clear about purpose and use

The Data Protection and Use Policy (DPUP) helps agencies fully understand and carefully explain their purposes of collection from the start.

Use personal information only for the collection purpose

Ordinarily, personal information should only be used for the purpose it was collected for unless another proposed use is permitted by:

- the exceptions in the Privacy Act 2020's information privacy principle (IPP) 10 — Limits on use of personal information
- a specific statutory provision.

IPP10: Limits on use of personal information — Office of the Privacy Commissioner

As the Office of the Privacy Commissioner (OPC) observes, the "effect of [IPP10] is to ensure agencies are accountable for their actions when collecting information by prohibiting them from 'repurposing' information".

This makes it important for collection agencies to fully understand and carefully explain their purposes of collection at the outset. Agencies need to ensure their genuine proposed uses are covered, while always bearing in mind they should not collect personal information if:

- it is not reasonably necessary for lawful purposes connected with their functions or activities, or
- the collection is under a specific statutory collection provision, and the collection exceeds the bounds of the provision.

It is generally acceptable for an agency to have and communicate more than one purpose for collecting personal information if, at the time of collection, it genuinely proposes to use the information for more than one purpose. All stated purposes must be lawful purposes connected with the agency's functions or activities.

However, it is not acceptable for agencies to include vague catch-all purposes to 'hedge their bets' that they might want to use the information sometime in the future. Agencies need to be able to show that the stated purposes of collection cannot be carried out without the collected information. Otherwise they run the risk of acting unlawfully.

In addition, collecting people's information and then doing nothing of value with it can erode people's trust and confidence in the collecting agency.

'Directly related purpose' exception relies on a clear original purpose

Under IPP10, personal information can only be used for another purpose if an agency believes on reasonable grounds that one of the IPP10 exceptions applies.

An exception is that the purpose of using the information is directly related to the purpose the information was obtained for. If an agency has not clearly defined the original purpose of collection, relying on this 'directly related purpose' exception could be difficult.

> Sometimes people wonder if a proposed use is directly related to the purpose the information was obtained for. The OPC has a useful summary of what needs to be considered.
>
> Where can I use the directly related purpose exception? — Office of the Privacy Commissioner

Clarity of other purposes also important

If an agency wishes to use personal information for a purpose other than the original purpose of collection, it's important the agency is clear about and documents the nature and scope of that other purpose. There are 2 reasons for this:

- to ensure that the other purpose is lawful by checking it against either IPP10 or, if a specific statutory provision authorises other uses, against that provision
- to have a record of the purposes personal information is being used for and why each kind of use is allowed.

If the documented other purpose is not lawful under either IPP10 or a specific statutory provision, then the personal information should not be used for that other purpose.

Purpose of proposed 'alternative use' needs to be clear

There are various contexts in which specific statutory provisions authorise the use of personal information for purposes that are different to the original purpose of collection.

Example 1

Under Section 126 of the Housing Restructuring and Tenancy Matters Act 1992, the Ministry of Social Development may use information obtained under a part of that Act, in its role as social housing agency, to perform its functions, duties, and powers under the Social Security Act 2018. Even here, the purpose of a proposed alternative use needs to be clear before relying on the specific statutory provision. This ensures the use is covered by the provision.

If an agency is not clear about the purpose of its proposed alternative use, then that use may not be covered by the provision and be permitted under IPP10. In that case, the agency's use of the information (depending on the circumstances) could be an 'interference with privacy' under the Privacy Act 2020.

Example 2

An 'interference with privacy' occurs where, for example, there is a breach of an IPP in the Privacy Act 2020 and that breach causes one or more individuals to suffer harm.

Be clear about purpose for sharing

The Data Protection and Use Policy (DPUP) helps agencies understand the importance of purpose to inform what's appropriate if they are thinking about sharing people's personal information with others.

Clear purpose required for sharing personal information

Being clear about purpose when collecting personal information can be relevant to whether an agency can share that information with others. This is because, under the Privacy Act 2020's information privacy principle 11 (IPP11) — Limits on disclosure of personal information, an agency must not disclose the personal information unless it believes, on reasonable grounds, that one of the listed exceptions in the IPP applies.

The first exception is that the disclosure is one of the purposes the information was originally obtained for or is directly related to those purposes. To determine if this exception applies, an agency must know the original purposes for obtaining the information.

If one of the purposes of collecting personal information is to share it with another agency for a particular reason, then the collecting agency needs to be clear about that upfront. If it will be shared with an agency overseas, the collecting agency needs to assess if sharing would be consistent with IPP12 — Disclosure of personal information outside New Zealand.

If collecting the information directly from service users, under IPP3 — Collection of information from subject, an agency needs to explain what agencies the information will be shared with and why. This is the case unless an

exception under IPP3 applies — for example, if it would undermine the purpose of the collection, or it's just not possible to tell the person.

If using information collected by another agency, the collecting agency needs to say who they will be sharing the information with and why. This may influence whether the collecting agency or organisation:

- is willing to disclose the information
- may seek to impose controls on further distribution of the information, for example, under a memorandum of understanding or contract.

Find more information on the information privacy principles:

IPP3: Collection of information from subject — Office of the Privacy Commissioner

IPP11: Disclosure of personal information — Office of the Privacy Commissioner

IPP12: Cross-border disclosure — Office of the Privacy Commissioner

If disclosure appears to be authorised by a specific statutory provision

IPP11 can be overridden by specific statutory provisions that either authorise or require the disclosure of personal information to other agencies. This is common in the social sector.

However, purpose remains relevant in this context as well. Usually such precise statutory provisions specify what purposes particular personal information can be shared for. This means the agency needs to be clear about the intended purpose of disclosure before relying on a specific statutory disclosure provision. This ensures the intended purpose of disclosure is covered by the provision.

If an agency does not define the intended purpose properly, its disclosure may amount to an interference with privacy if the disclosure:

- was not covered by the provision
- would not have been permitted under IPP11 either.

Assess purpose and only collect what is needed

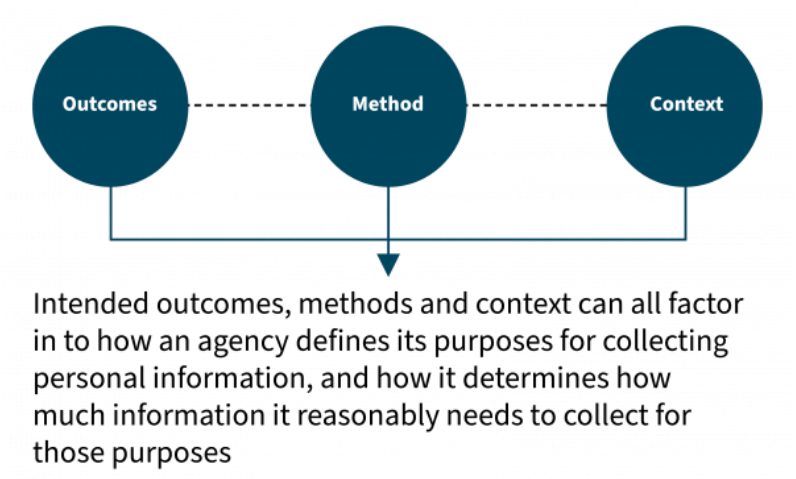
Agencies should assess the purpose of collecting personal information to ensure they are collecting only what's needed.

Assess the purpose for collection

When assessing the purpose of collecting personal information and the kinds of information to be collected, agencies should:

- be clear about the outcomes to be achieved
- be clear about the method that will be used to achieve the outcomes
- consider in what context the information will be collected and used.

Diagram 1: Intended outcomes



Detailed description of the diagram.

Diagram shows 3 circles labelled 'Outcomes', 'Method' and 'Context' connected by dotted lines pointing to the text that explains that these can all factor into how an agency defines its purposes for collecting personal information, and how it determines how much information it reasonably needs to collect for those purposes.

Clarity in these areas can help an agency to:

- formulate the purpose of collection
- assess if that purpose relates to the agency's functions or activities
- assess what personal information is needed to achieve the outcome
- determine if the collection is ethically justifiable and aligns to respectful practice (even if it will tick all legal boxes).

Be clear about the outcomes

To have clarity of purpose it's necessary to understand why data or information is being collected — that is, the outcome or result of using it.

This should be well-defined and easy for a range of people, including service users, to understand. It should be written down. Recording it:

- helps agencies to think clearly
- captures information that needs to be communicated to service users — either directly, if the collecting agency is collecting the information directly from services users, or through another agency that is collecting the information from service users
- provides the basis for the collecting agency to determine if proposed future uses or disclosures of the information are for a purpose it was collected for or a directly related purpose.

Without clarity, an agency may not be able to determine if it's necessary to collect the information it proposes to collect. In that event, the agency's collection may breach the Privacy Act 2020's information privacy principle 1 (IPP1) — Purpose of collection of personal information or, where relevant, not fall within a specific statutory collection power the agency is aiming to use.

IPP1: Purpose for collection of personal information — Office of the Privacy Commissioner

Who the outcomes serve

When considering the outcomes, it can be helpful to reflect on who the outcomes serve:

- Do the individuals the information is collected from benefit, or do other people or does wider society benefit?

- If the benefit is to other people or wider society, what will the people providing the information think about that?
- Even though the Privacy Act 2020 or a specific statutory provision may allow the collecting, is using the information to benefit others ethically justifiable?

Be specific about what the information will be used for

Agencies need to avoid broad and ambiguous statements of purpose or outcomes. If your agency is collecting information for analysis, policy development or service design, either by itself or in conjunction with other data, you should describe these uses as precisely as possible.

If the results will be used to provide more targeted services and better outcomes for people, then say that, being as precise as possible.

If the results could lead to taking adverse action against people, say that too.

Consider telling people what their information will not be used for

IPP3 — Collection of information from subject — is concerned with telling people about the purposes for which their information will be used. That makes sense, especially when other uses are not permitted unless either an exception in IPP10 — Limits on use of personal information — applies or a separate statutory provision authorises another use. However, agencies cannot expect service users to understand this legal position.

IPP3: Collection of personal information from subject — Office of the Privacy Commissioner

IPP10: Use of personal information — Office of the Privacy Commissioner

> - It can sometimes be helpful to explain to people that, while their information will be used for purposes A and B, it will not be used for purposes X or Y. For example, if your agency is collecting particularly sensitive information about people to provide them with immediate care, and there's no intention to allow any identifying information to be seen by researchers or other agencies, you could say that.
> - Similarly, if the information you're collecting includes unique identifiers like a driver licence number, IRD number or passport number, you might want to tell people their number will not be used to match information you have about them with information another agency has about them. Deciding if it's a good idea to make statements like this will depend on the context.

This consideration can be particularly important where people may fear their information will be used in a prejudicial manner against them. Taking this approach can help increase people's levels of comfort with what's happening with their information.

Be careful with evolving purpose statements

When a policy, service or programme is evolving, an agency may change or refine how it articulates the purpose of a proposed collection before collecting the information. If so, the agency should:

- be clear about which purpose statement is the final one
- state if the final statement is intended to replace earlier explanations.

Having different explanations of the purpose of collection across different policy, service or programme documents can lead to confusion about what the actual purpose of collection is or was. This could result in errors when explaining to people why the information is being collected and how it will be used.

It could also result in service users losing trust in the agency. If there is cause for an investigation into the purposes of collection, different purpose statements over time could result in uncertainty and adverse findings.

Be clear about the method

Why the method is important

As well as having a clear understanding of the outcome, it's important to consider the method to achieve the outcome. Both the end and the means are important.

Knowing how the information will be processed to achieve the outcome can be relevant to determining if the information being collected can or will contribute to the outcome and, therefore, whether all of it is required to achieve the outcome.

Example

An application form for a service might collect personal information such as a person's name, date of birth, annual income, address, gender and ethnicity.

However, a tool to process such applications, and designed to match the eligibility criteria for the service, may only need name, date of birth, address and annual income. The agency may have no plans to use the information relating to gender and ethnicity. In that kind of situation, collecting information on gender and ethnicity would be unnecessary and, in all likelihood, unlawful.

Consider different analytical techniques or processes

In some situations, there may be different analytical techniques or processes for achieving an outcome. To achieve the outcome, the different techniques or processes may require more or less personal information, or even no personal information at all (because, for example, it can be de-identified before collection).

If one technique requiring less personal information can easily be deployed over another that requires more personal information, respectful practice means choosing the former technique to minimise the amount of personal information collected.

If a collecting agency needs to know people are over 20 years of age, it might use a tool that asks for a person's date of birth or age but then uses that to work out if the person is over 20 and only stores a 'Yes over 20' response, instead of the date of birth or current age.

Collecting agencies that need help with this can reach out to others with relevant experience or expertise. Depending on the context, it might be helpful to seek advice from other agencies such as Stats NZ, frontline non-governmental organisations (NGOs), service user representatives, the Office of the Privacy Commissioner or the Government Chief Privacy Officer.

Should agencies collect personal information from every service user all the time

In some situations, an agency may propose to collect information from a wide group of people to achieve a stated purpose or outcome. However, the group may have different subgroups or be made up of people with different service needs, sensitivities or fears.

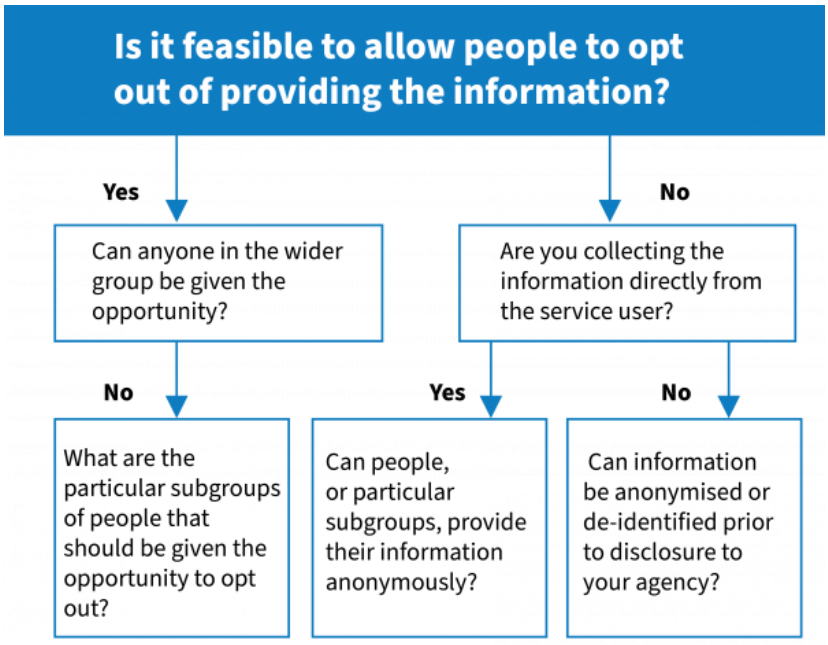
At a macro level, it may be reasonable to conclude that it's reasonably necessary to collect personal information from members of the wide group of people to achieve the stated purpose. However, it does not necessarily follow that the information needs to be collected from every member of the group, all the time, and regardless of individuals' different service needs, sensitivities or fears. That depends on the context.

The key point is to consider whether the purpose can be achieved if only a proportion of people in the group provide the information requested. If the answer is yes, it may be helpful to assess whether allowing people to opt out of providing the information is feasible. If it is, the collecting agency can then consider whether anyone in the wider group should be given this option or whether there are particular subgroups of people, for example, vulnerable people needing services for particularly sensitive issues, that should be given the opportunity to opt out.

If opting out is not feasible, another option might be to allow people, or particular subgroups, to provide their information anonymously. Or, if the collecting agency (Agency A) is collecting information from another agency or organisation (Agency B) that collects personal information directly from individuals, it may be possible for Agency A's

purposes to be achieved by collecting information from Agency B that has been anonymised or de-identified prior to disclosure to Agency A.

Diagram 2: Is it feasible to allow people to opt out



Detailed description of the diagram.

The diagram is a flowchart that starts at the top with the text on a blue background: "Is it feasible to allow people to opt out of providing the information?" From this text, 2 blue arrows point downwards representing 2 options 'Yes' and 'No'. The first option / arrow with the word 'Yes' against it points down to a box containing the words: "Can anyone in the wider group be given the opportunity?" From this box, a blue arrow with 'No' against it points downwards to a box containing the words: "What are the particular subgroups of people that should be given the opportunity to opt out?"

From the top text box, the second option / arrow with the word 'No' against it points down to a box containing the words: "Are you collecting the information directly from the service user?" Two blue arrows point downwards from this box representing the options, 'Yes' and 'No'. The first option / arrow with the word 'Yes' against it points down to a box containing the words: "Can people or particular subgroups, provide their information anonymously?" The second option / arrow with the word 'No' against it points down to a box containing the words: "Can information be anonymised or de-identified prior to disclosure to your agency?"

When IPP1 applies, these considerations are directly relevant to whether the collecting agency can conclude that it's always reasonably necessary to collect the personal information from everyone, all the time.

The wider and more diverse a group is, or the longer the period of information collection is likely to be, the more important this question may become.

If agencies collect information from one channel or into 1 repository

Sometimes agencies collect different kinds of personal information for different purposes but through a single collection channel and into a single location. In other situations, an agency might use different collection channels but collate all the information into a single repository or output, such as a spreadsheet.

If there are several groups within an agency who need to have access to different kinds of personal information, having all the information in 1 location or repository could result in some staff having access to personal information they do not need to see and which, therefore, they should not see.

This could also be contrary to IPP5 — Storage and security of personal information. Under IPP5, agencies need to ensure that personal information they hold is protected by reasonable security safeguards "against ... access, use, modification, or disclosure that is not authorised by the agency".

In this kind of situation, part of the method for achieving the outcomes (that is, the means for collecting and collating the information) may be inappropriate and needs to be reconsidered. This can be particularly important as service users can get understandably worried about too many or the wrong people having access to their personal information.

IPP5: Storage and security of personal information — Office of the Privacy Commissioner

Consider the context

Relevance of context

Context matters because it influences how people might feel about the collection or use of their personal information for particular purposes or how much information is collected, and that, in turn, may affect their wellbeing.

It also affects the kinds of checks and balances an agency may decide to work through before collecting, using or sharing personal information for a particular purpose — especially if there's any risk that collecting, using or sharing personal information in the manner proposed could do, or be perceived to do, more harm than good.

Context can also be relevant to the collection, use or sharing of information that has been de-identified, in the sense that it will not be possible to identify specific individuals from the de-identified information. This is because de-identified information can still contain information that some individuals, groups or cultures may find sensitive.

> It can be particularly important to remember that, while the Privacy Act 2020 is concerned with the privacy of individuals, we live in a society where broader groups have legitimate privacy interests.
>
> The Privacy Act 2020's controls may fall away once personal information has been fully de-identified in the sense described above, but the remaining information could still be sensitive to, for example, whānau, hapū, iwi, Māori, other cultural groups or other societal groups.

The next part of this Guideline provides guidance on potentially relevant contextual matters and describes some specific issues that may be particularly important in some situations.

Questions to consider

The following are some contextual matters to consider in decision-making.

Who collects the information from service users?

- Will your agency collect the information from service users? If not, which agency will or did collect it from them?
- If another agency will or did collect the information you want to use, will the service users be told, or were they told that your agency would receive their information?
    - If not (and assuming the original collecting agency is permitted to disclose it to your agency and that your agency is permitted to collect it), how might they feel about your agency having their information? Could your agency's use of their information be distressing to them or otherwise adversely affect their wellbeing?

What type of service does the information relate to?

Generally speaking, the more sensitive, urgent or acute a service is for people, the more important it becomes to take people's wellbeing into account when considering:

- the purposes their information will be collected for (especially if those purposes entail disclosures to others)
- how much will be collected.

Example

An agency provides a support service to victims of serious crime. The nature of that service and what the victims have experienced are highly relevant to:

- the purposes their personal information might be collected for
- how much personal information might be collected
- how their personal information might be used and shared with others.

This is the case regardless of what the law may permit.

What is the nature of the information?

- Is the information fairly routine or basic in nature or is it particularly sensitive? For example, is it about service users' mental health or their attendance in a programme? Consider that, in some situations, information that may sound fairly routine to the collecting agency may actually be quite sensitive for the people asked to provide it.
- If information is collected in circumstances where those providing it do not need to establish their identity, is there a risk of receiving inaccurate information?
- Is there any potential for people to feel judged or discriminated against by an agency using their information in the proposed manner?
- Would the collection or use of the personal information affect people's trust and confidence in the agency collecting it or using it?

What are the circumstances of the people involved?

- Might the proposed use of service users' personal information be seen as unrepresentative or reinforcing of stereotypes?
- Is the information about children, people who are marginalised or stigmatised, or people at greater risk of harm, and whose information needs greater protection?
- If the information comes via a service or programme, do the people concerned self-refer or is their attendance compulsory?
  This may influence how much choice they have over the collection of their information and how they might feel about that or about it being used for other purposes, even if they're told about those other purposes when their information is collected.

What is the potential for adverse consequences?

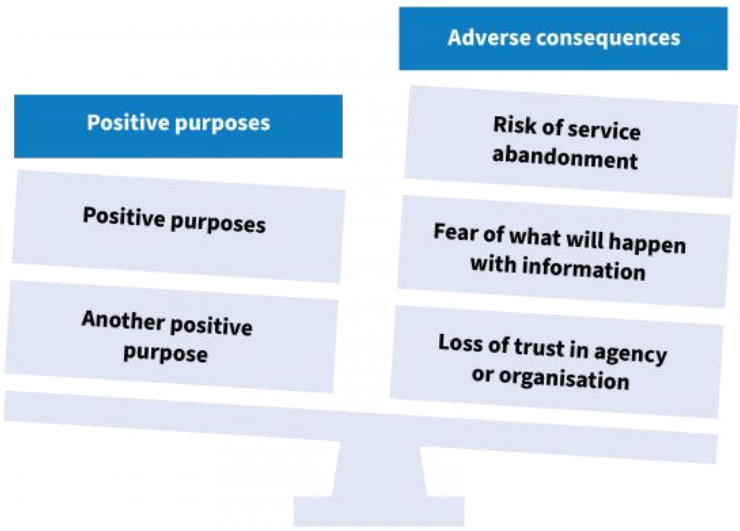
An agency's purpose for collecting personal information may be related to its functions or activities, and be well-intentioned, and understandable. The collection of personal information to achieve that purpose may appear to be reasonably necessary. It may be consistent with government priorities and policy objectives and, from these perspectives, justifiable. From a legal perspective, it might tick all boxes under IPP1.

Applying the Data Protection and Use Policy (DPUP) He Tāngata Principle, though, means asking whether pursuit of the purpose and the collection of personal information for that purpose could have adverse consequences for people. This is where the Privacy Act 2020's IPPs are relatively silent. Indeed, there can be instances where a collection and use will not be contrary to any privacy principle but where the potential for adverse consequences, once understood, may prompt reconsideration.

In some situations, particularly where new policies, services or programmes are involved, it may be desirable to consider the ethical considerations of what is proposed. For example, it may be desirable to:

- take both the positive outcomes and the potential adverse consequences into account before proceeding, and to ask if pursuit of this purpose could do more harm than good, even if that's not the intention
- consider the importance of respecting people's dignity and treating them in a just manner, consistent with the He Tāngata Principle.

Diagram 3: Positive purposes versus adverse consequences scale



Detailed description of the diagram.

A set of scales with the higher end balancing 3 boxes labelled 'Positive purposes', 'Positive purposes' and 'Another positive purpose' against 4 heavier boxes labelled 'Adverse consequences', 'Risk of service abandonment', 'Fear of what will happen with information' and 'Loss of trust in agency or organisation'.

Sometimes, it can help to imagine what is proposed like the scale in Diagram 3. This is a simple representation of what will often be a complex picture (in an actual situation, the positive purposes would be specifically described, and there could be additional or different adverse consequences) but it may help to put matters in perspective and prompt a collecting agency to ask if it has only been thinking about one side of what lies in the balance.

Identifying the adverse consequences may also help an agency to take steps to avoid them while still enabling it to pursue one or more of its original purposes.

Example

Agencies require information from people or from service delivery organisations who collect information. However, if people are afraid of what might happen to them or who might see their sensitive information, they could walk away from services they need. This situation might result in more harm than good. Even when lawful, agencies may need to take care to ensure information collection practices do not deter people from seeking the help they need.

How could linking people's personal information with other data be perceived?

It is not uncommon for personal information to be collected with a view to linking it with other datasets to yield insights, whether as the sole purpose of collection or as one of the purposes of collection.

If a collecting agency proposes doing this, it needs to be clear about the nature of the proposed linking and how resulting insights will or are likely to be used. This is important to avoid over-collection of personal information and to be able to explain to people how their personal information will be used.

While the law allows this kind of linking in certain situations (each situation needs to be assessed on its merits), it can be important for the collecting agency to ask itself, and sometimes service provider organisations and service users, what people would think about their information being linked up in this way.

This question remains important even when the resulting data will be de-identified or anonymised before further use as some people may still have concerns about information derived from their personal information being used in this way, particularly where the information is sensitive.

If the collecting agency elects to proceed with the collection for linking purposes, the next question needs to be considered.

What should an agency tell people about their personal information being linked with other data?

This topic is part of the Transparency and Choice Guideline, but it is mentioned here as well, given its relationship to the purpose of collection.

> From an ethical perspective, and bearing in mind the nature and range of information that circulates among agencies, it is important to explain to service users their data may be linked with other data, regardless of whether the law requires that.
>
> This is not a straightforward point because, under IPP3, one of the grounds for not having to explain the purposes of collection and other matters to people is where the agency believes that the information will be used for statistical or research purposes and will not be published in a form that could identify individuals. If an agency's linking purposes fall squarely within this exception, it might conclude that it does not need to tell people about the linking and how the insights will be used.

However, there is nothing sufficiently unique about collecting personal information for statistical or research purposes to justify not telling people that their personal information will be linked with other datasets to yield insights, even where an agency can rely on the IPP3 exception.

What is the potential impact on relationships when personal information is collected from other agencies?

People form trust relationships based on interactions they have with other people. When information is collected by frontline service delivery organisations, such as NGOs, those trust relationships may exist at the local level. They may have developed over time and they may be based on particular approaches to, for example, information disclosure and consent, that the service delivery organisations have followed. In some cases, these approaches may have flowed from codes of ethics that certain service providers need to follow as a matter of professional obligation.

If an agency is proposing to collect personal information from frontline service delivery organisations, it can be important to:

- take existing trust relationships and approaches into account
- ask what impact the agency's collection from these organisations could have on them and their clients.

It may be important to consult with the organisations and, where appropriate, service users, at an early stage, before collection decisions are made

Work through checks and balances

It's important agencies check their purpose for collecting people's information and whether it is appropriate or required.

When to work through checks and balances

The Data Protection and Use Policy (DPUP) Purpose Matters Guideline emphasises the importance of:

- getting the purposes of collection right
- only collecting what's reasonably necessary for those purposes
- taking care to avoid unintended adverse consequences.

To achieve this, agencies should use checks and balances described in the section 'Suggested checks and balances' below, to test their initial thinking around information collection – what's their purpose and is it necessary or appropriate.

It is important to do this when an agency:

- is unsure about how it is articulating the purpose of collection, for example whether it's precise enough and covers all genuine purposes or whether it could lead to overcollection of personal information
- identifies a risk that others, particularly service delivery organisations and service users, could be concerned about
- is unsure whether the purpose of collection is sufficiently connected to the agency's functions or activities
- operates in a complex legislative environment — that is, in addition to the Privacy Act, an agency has powers or is subject to constraints in specific legislation that applies to that agency
- proposes to collect sensitive information or information that could be perceived to have no logical connection to the stated purposes
- is considering information that could be used to discriminate against people, for example, gender, marital status, ethnicity, religious belief, sexual orientation, or mental or other health information
- is collecting the information or using it for a stated purpose in a manner that could adversely affect the trust and confidence people have in the agency, or run the risk of people in need not asking for the help that's available to them.

Agencies should also note that poorly written purpose statements could result in:

- service users or other agencies complaining
- the Privacy Commissioner enforcing measures.

Under the Privacy Act 2020, the Privacy Commissioner can issue a compliance notice if they believe one of the Privacy Act 2020's information privacy principles (IPPs) has been breached, for example, IPP1 on the purpose of collection or IPP3 on what a collecting agency needs to tell individuals.

A compliance notice describes the breach and requires the agency to remedy it. It can be issued if no harm has occurred.

IPP1: Purpose for collection of personal information — Office of the Privacy Commissioner

IPP3: Collection of information from subject — Office of the Privacy Commissioner

Suggested checks and balances

To ensure that its purpose of collection and its privacy statement are clear and comply with the Privacy Act 2020, an agency may wish to seek:

- input from a privacy consultant
- legal advice from a lawyer with a solid understanding of privacy law
- advice from an appropriate review group or panel if ethical questions arise, for example, Data.govt.nz's Data Ethics Advisory Group
- input from other agencies including, where relevant, service delivery organisations who have a relationship with service users
- information from service users or service user representatives.

What is a privacy statement and what to include — Office of the Privacy Commissioner

Agencies may also wish to:

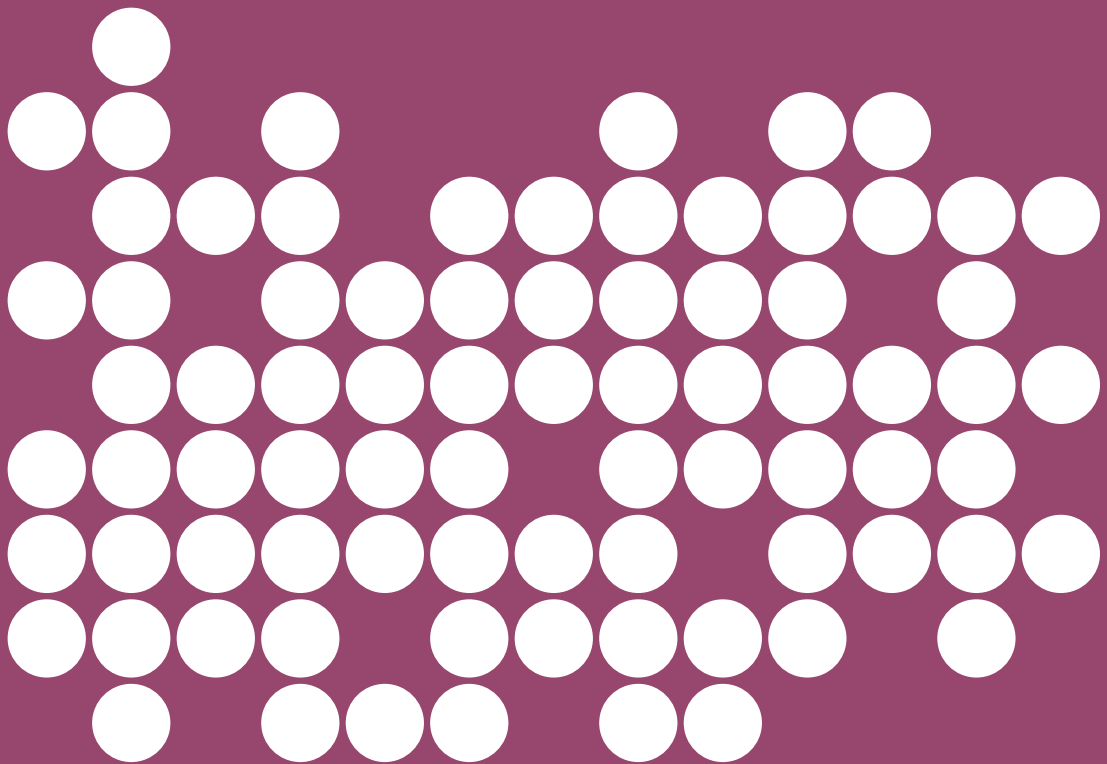
- check with a line manager, and get their opinion
- ask the agency's privacy officer for help
- undertake a privacy impact assessment or, if available, apply a framework like the Ministry of Social Development's Privacy, Human Rights and Ethics (PHRaE) framework (PDF 258KB)
- raise any risks or uncertainties about the proposed purposes of collection and the information to be collected with the agency's executive management team
- consult relevant Māori groups if the collection or use could have a distinct impact on Māori, or raise concerns for Māori

- consider whether to establish or seek advice from a review board, external reference group, ethics committee or client reference group
- consult the Office of the Privacy Commissioner.

Guideline

Transparency and Choice

Help people understand why and how providing personal information can help them or people in similar circumstances, if providing some information is optional, and their rights to access or request changes.



Transparency and Choice Guideline

Why DPUP has a Transparency and Choice Guideline?

Help people understand why and how providing personal information can help them or people in similar circumstances, if providing some information is optional, and their rights to access or request changes.

Transparency and Choice's intent

The Data Protection and Use Policy (DPUP) Transparency and Choice Guideline helps agencies make it easier for service users to understand and, where possible, have choices about when and how their information is collected and used.

Having this understanding and choice improves people's trust in agencies collecting and using their information. The steps described in this Guideline also help to ensure that information is accurate and relevant for its intended purpose.

Service delivery organisations collecting personal information, and service users themselves, stress the approach must be open and honest. Clear guidance in this area helps agencies that collect and use people's information to:

- find ways, where possible, to give people choices about what information is collected and how it's used, while still enabling the purpose to be achieved
- avoid using the language of consent if it suggests people have a choice when they may not, or if their only real choice is between using or not using a service they need
- be transparent and ensure understanding about what information is collected, why and how it may be used
- explain what happens to information if and when it is used beyond frontline assessment or service delivery.

Transparency and Choice's key concepts

This Guideline describes an approach that focuses on transparency and openness as the foundation of improved trust.

It describes collaborative responsibilities for agencies to ensure that service users can understand what happens with their information in a way that makes sense to them and their circumstances. This includes opportunities to further develop that understanding over time.

The Guideline also outlines how this might be done in a manner that respects people's mana.

Important reasons for this Guideline

- People who use agency services want a good understanding of why their information is needed. When they're unclear about it, this can cause anxiety, especially if their current situation is already a difficult one.
- When seeking support, service users who are in crisis may not be able to fully understand what is happening with their information. They may express an interest later.
- Service providers and service users are clear that it's important people know what information is held about them, have a say about how it's used and who gets to see it, and are confident the information is accurate.
- Frontline professionals are clear that explaining how you use people's information, or gain their consent to use it, directly influences building relationships of trust.
- Service users sometimes express concern that their information could be used against them or their whānau without their knowledge. For example, if it is disclosed to other agencies who may judge them or make a decision that negatively impacts them.
- Service users understand the potential value their information has to enable better outcomes for people in similar circumstances. They want to be confident their information will be valued, protected, respected and used in accordance with that potential.

- An individual's circumstance is important in ensuring understanding and choice. For example, age, culture, language and literacy must be considered, as well as any other circumstance that is relevant to respecting mana and enabling understanding of their choices.

It's also important to remember the context of particular people and communities.

- Māori providers and other Māori / iwi groups want te ao Māori considered when Māori communities are a key focus.
- Pacific peoples are looking for clear and simple explanations in language they understand about why their personal information is being collected and how it will be used. They are also looking for greater accountability to families and communities on how their data is used.
- Disabled people also highlight the need for clear and accessible information about what information is being collected, and for what purpose. Disabled people want a greater understanding of people's situations when asking for identification information. For example, some disabled people do not have a driver licence.

Using the language of choice

This Guideline uses the language of 'choice' rather than 'consent'.

- Consent is given when a person voluntarily agrees to something based on a good understanding of the consequences.
- Choice gives people control, whenever possible, over what information they decide to provide.

Agencies often use the language of consent, but without common agreement about what it means. Consent can have specific definitions in fields such as medicine, research and law. It is often used in circumstances where people who want to access an agency will not receive the help they need if they don't provide the information requested.

For this reason, DPUP uses a plainer word — choice — and focuses, in part, on the processes that help give people choices and allow them to act on those choices.

This language also reflects the fact that the Privacy Act 2020 is not consent-based privacy legislation.

Help people to understand

The Data Protection and Use Policy (DPUP) gives agencies advice to help people understand what information they're being asked to provide, and why.

What people need to be made aware of

Under the Privacy Act 2020's information privacy principle 2 (IPP2) — Source of personal information, agencies that collect personal information need to collect it directly from the people concerned unless an IPP2 exception applies. This means agencies can ensure they are transparent with people about collecting their information because they are dealing directly with the people.

In addition, information privacy principle 3 (IPP3) — Collection of information from subject, sets out what agencies must make people aware of when collecting their personal information.

IPP2: Source of personal information — Office of the Privacy Commissioner

IPP3: Collection of information from a subject — Office of the Privacy Commissioner

> This Guideline proposes that 'ensuring people are aware' should mean helping them reach a reasonable understanding in a way that makes sense to them at the times that work for them.

The focus of IPP3's transparency requirements is on ensuring people are aware of:

- what information will be collected from them
- why it's needed (the 'purpose' of collection)
- what choice they have over its collection.

Ideally, this level of understanding should be achieved before the information is collected, but this may not always be possible (or 'practicable', as IPP3 puts it). Where it's not, the agency needs to make people aware 'as soon as practicable' after collecting their information. What is practicable will depend on the situation, including the person's circumstances and the nature of the service that person needs.

The specific matters that people need to be made aware of are:

- the fact that information is being collected, what information is being collected, and why (the purpose their information is needed for)
- who will receive (or be able to see) their information: Provide clarity about who sees personal information
- if the collection is authorised or required by law, what that law is, and if people can choose whether to provide the information
- what the consequences might be if someone does not provide the information requested
- people's rights to access and to request correction of their information.

When agencies do not have to make people aware

There are some limited circumstances where an agency that's collecting personal information from people does not need to make them aware of these matters. An agency does not need to if it has already done so in relation to the same kind of personal information in the recent past.

The agency also doesn't need to if it believes on reasonable grounds that:

- not providing that information
  - would not prejudice the interests of the individual concerned
  - is necessary (in the case of a public sector agency) to uphold or enforce the law, protect the tax base or assist court or tribunal proceedings
- providing that information
  - would prejudice the purposes of collection
  - would not be reasonably practical in the particular case
- the personal information collected from the individual concerned will not be used in a form in which the individual is identified or will be used for statistical or research purposes, and will not be published in a form that could reasonably be expected to identify the individual.

> Reliance on these grounds is the exception rather than the norm. The default is to provide people with the information required by IPP3. It's also important to note that many of these exceptions must be considered on a case-by-case basis and do not justify non-compliance with IPP3 for a broad group of service users.
>
> If an agency does not inform people of the matters listed in IPP3 and none of the grounds above applies, the Privacy Commissioner could issue a compliance notice to the agency that describes the breach of IPP3 and requires the agency to remedy it. Compliance notices can be issued in the absence of harm.

What agencies should also consider

While the Privacy Act 2020 does not require agencies to do these things, it is also good practice to explain:

- how people's privacy will be protected, in terms of safe storage and security of their information and the access controls it will have that is consistent with the agency's obligations under IPP5 — Storage and security of personal information
- how the information will be used to help them or people in similar situations to them (if this is not already part of the communicated purposes of collection) and, where possible, examples of this happening
- if the collected personal information will be matched or linked with other data relating to the same individuals, particularly data sourced from other agencies, the fact that matching or linking will occur, why it is being done and what it could mean for those people

- if relevant, how particular information may be used in a form that does not identify them. People often think of their information as being about them even if it does not identify them and like to know how the information they provide will be used even when identifiers are removed or masked.

IPP5: Storage and security of personal information — Office of the Privacy Commissioner

> Under the Privacy Act 2020's IPP3(4)(e)(i), an agency does not need to tell people about a collection of personal information, its purpose and the other matters listed in IPP3 if the agency believes on reasonable grounds that the information will not be used in a form in which the individual concerned is identified. It may still, however, be good practice for the agency to tell them.
>
> Part 3 of the Privacy Act 2020: Information privacy principles and codes of practice — Parliamentary Counsel Office

Provide clarity about who sees personal information

The question of who can see the often sensitive personal information collected from service users is an important one. This is particularly so if a collecting agency is large and has many different functions, and may share personal information with other agencies.

IPP3 refers only to making people aware of the "intended recipients of the information". This phrase does not distinguish between recipients. For example, it may mean:

- different people or groups within the agency collecting the information
- different agencies of any kind that may receive the information.

In addition, in the past, the Office of the Privacy Commissioner (OPC) has said it does not require the collecting agency to list every possible person it might pass personal information to — it will be enough to give a general idea of who is likely to see the information and why they might see it.

IPP3: Collection of information from subject — Office of the Privacy Commissioner

At the same time, it's also clear the OPC considers it can be appropriate to inform people of:

- any other agencies the information may be shared with
- the kinds of people within the collecting agency who will see their personal information.

This Guideline takes the same approach. It's an important point because this part of IPP3 is often read as relating only to sharing personal information with other agencies.

This can result in little or nothing being said, in privacy statements, for example, about the limited audiences within the collecting agency who can see people's personal information and that, in turn, can cause worry and concern for service users.

> In general, the larger and more multifaceted a collecting agency is, the more important it becomes to explain to service users who within the agency will and will not have access to their personal information. What can be said will depend on the situation and who within the agency may need to see the information.
>
> It's important to not leave people with the impression that anyone inside the agency will be able to see their personal information, especially when they do not have a genuine need to see it.

Help frontline staff to help service users understand

For a range of reasons, sometimes those collecting personal information directly from people do not know all the reasons why it's being collected. This is because the decisions about what to collect may have been made by others in their agency, or in parallel with or by another agency. In other words, there can be a knowledge gap between those deciding to collect and those who do the collecting.

Anyone involved in designing information collections or communicating them to others, for example, in contracting documents, needs to help ensure that everyone involved, including those dealing directly with service users, has a

good understanding of the 'what and why' as outlined in this Guideline. Not doing this may undermine people's responsibilities, which often flow from legal duties that agencies have to service users.

If those dealing directly with service users do not have a good understanding of why information is being collected, they may not be able to prepare their privacy statements, explain matters proactively or answer service users' questions.

> If you're collecting personal information from other agencies they need to understand your purpose of collection. At the same time, those involved with collecting service users' personal information and, where relevant, those being asked to share it with other agencies, need to feel able to ask 'why', safely and confidently, and without fear of negative consequences.
>
> People involved in the chain of collecting, using and sharing information have a right to be given a good answer. Agencies should assume that at some point a service user will ask the same question.

When other agencies need to understand the purpose of collection

Agencies have accuracy obligations

Agencies have a responsibility under IPP8 — Accuracy of personal information — to be checked before use or disclosure, to take reasonable steps before using or disclosing personal information to ensure it's accurate, up to date, complete, relevant and not misleading.

Helping service users to have a good understanding of what's being collected and the purposes of collection, while proactively providing them with means to access and request correction of their information (or to correct it themselves), can help agencies meet their own obligations under IPP8.

Service users may be more likely to request corrections of their personal information (or, if possible, update it themselves) if they think it's inaccurate or incomplete.

IPP8: Accuracy of personal information — Office of the Privacy Commissioner

Match the approach to the context

Consider how to provide good, safe opportunities for service users to understand and ask questions about the collection and use of their personal information. Think broadly about how you approach this.

Consider a range of methods

It can be helpful to consider a variety of ways you could explain the collection and use of their personal information to your service users. These might include:

- one-to-one conversations
- brochures, factsheets or FAQs to take away
- posters in offices
- website information at different levels of detail
- information on forms they are asked to sign, and copies they can take away
- presentations to groups of people.

The most effective approach will often be to talk people through the collection and use of their personal information in person so they can ask questions.

While a range of different approaches can work, it's important to check with people from time to time to confirm their understanding of what's been discussed.

It's also important to respect and respond to cultural and language considerations.

Provide multiple opportunities for people

Service users will sometimes be stressed or in crisis when they initially look for support. They may not yet be interested, willing or ready to think about what may happen with their personal information. For that reason, it may be necessary to offer a number of opportunities to re-visit the topic, and to respond appropriately to their level of interest in understanding.

Service users in this kind of situation could include victims of crime, or children or young people whose authority or willingness to make decisions about themselves changes as they become older.

Example

In some situations, agencies might:

- inform service users face to face of key matters relating to the collection and use of their personal information,
- give service users a 1-page information sheet to take away
- tell service users they can check the agency's privacy statement on its website for further information about how their information is handled and who to contact if they have any questions.

Be specific and give clear explanations

The Data and Protection and Use Policy (DPUP) focuses on the importance of understanding.

When explaining about the collection and use of personal information, be as specific and clear as possible so people have the best chance of understanding what information is being collected, how their information will be used and who will be able to see it.

Note that both general and detailed information can be given in, for example, layered privacy statements. This approach can help people match their understanding to their interest.

Insufficient explanation	Better explanation
"We will share information with relevant agencies."	"We will share your information with agencies X, Y and Z for these reasons…"
"Information is used for service improvement."	"Your information might be used without your name, address or anything else that identifies you to help us apply for more funding."
"Information will be used for research purposes."	"This information about you will be linked with other information about you that we hold to help us research [XYZ], but anything that identifies you will be removed before anyone uses it for research."
"We will share your information with people who need to see it."	"People directly involved in providing services to you and our internal researchers will be able to use your information, but other people, for example, contract managers, will not be able to see it."

Things to consider

For information collection, consider:

- Will service users be surprised by anything if they come to understand or hear about it later?
- What are your service users' communication needs? What timing, language, format, visuals, flowcharts, pictures or other things could be helpful?
- Is this a one-off encounter or a long-term engagement when there may be further opportunities to discuss the information being collected and what may happen with it?

- What kind of information is being collected, what will it be used for and how might that impact what service users need to understand either now or over time?
- Does it make sense to provide detailed information or can more general explanations be used, given the variety of purposes and information collected?
  Think carefully about the balance, as generalisations can raise further questions and risk being inappropriate. Assumptions about how service users perceive the sensitivity of their information may not be accurate.
- If another agency is collecting information on your behalf, what support does it need? The collecting agency should be given the information it needs and feel able to freely ask all the questions that service users may ask it.
- Who can help to develop or test forms, explanations and other communication material?

If service users have questions or complaints, do you provide information about:

- who people should contact if they have questions? Do they know how to do that?
- their right to complain and how they can do that? For example, do you provide details of who they can contact, by email or phone? Do you provide an online contact form? Do you invite them to come and talk with you if they wish?

Make sure there is a safe and responsive environment

It's important people can get a good understanding of what agencies are doing with their personal information in a safe and responsive environment.

Ensure people feel safe

The Data Protection and Use Policy (DPUP) focuses on ensuring people understand what's happening with their personal information. It's helpful to consider how to ensure people feel safe so they are confident to ask questions when they need to.

Things to consider

- How will you ensure that people feel safe and confident to ask questions, either when information is first collected or at regular intervals?
- Appreciate that people read, hear, learn and understand in different ways. Be prepared to offer choices about how they want to understand things. Adapt information, processes and communication material to meet different service users' needs. For example, consider their Kaupapa Māori contexts, age, spoken languages and other factors that might suggest necessary alternatives.
- How can you check people's level of understanding and interest? Thinking about their personal information will not always be their first priority, but it will matter at some stage. Find ways to check they are achieving the required level of understanding. For some groups of service users, this might be achieved through sampling some users to check if the explanations are working for them.
- Consider if timing matters. When personal information is collected, the Privacy Act 2020 requires agencies to tell service users about the matters listed in information privacy principle 3 (IPP3) — about the collection and use of their personal information. If that's not practical (for example, they are in crisis or there is an emergency), agencies should tell them as soon as possible after that. In some situations, it may be appropriate to explain a minimum amount of information straight away and then follow up with the person with more detailed information later.

IPP3: Collection of information from subject — Office of the Privacy Commissioner

Offer choices when you can

When applying the Data Protection and Use Policy (DPUP), understanding a person's situation matters. Context can affect whether people should have a choice about providing personal information.

Understand the situation

People may have:

- **no choice** — for example, a person may be required by a specific statutory provision to provide personal information when requested by an agency they had already applied for a particular benefit or service from
- **limited choice** — for example, a person may need to accept that providing some level of personal information is an essential part of using the service in question, such as using a mental health counselling service (so the only choice is whether to accept the service or not)
- **some choices** — for example, a person may choose to enrol in a drug and alcohol support programme where they will have choices about what experiences they do or do not share, and with whom.

Even when it's not feasible for an agency to offer a person a choice about providing their information (for example, because the information is required to provide a requested service), it may still be possible to offer choices about:

- how the information is captured — for example, by a member of an agency's staff writing down what a person says versus giving someone a paper or online form to fill out
- who is able to see or use the information — for example, by enabling people to record their wishes about limiting access and respecting those wishes.

> It's important that people who need to access a service to improve their wellbeing, or the wellbeing of their whānau, understand how their information will be collected and managed and the benefits of providing it.
>
> When their only practical choice is to provide their information or refuse a service, having this understanding may help them to provide their information with confidence rather than refuse a service that could help them.

Identify choices

People who are involved in deciding what personal information may need to be collected for specific purposes should try to identify any choices that are consistent with the purpose and will not affect the outcome.

For example, cultural considerations or the fact that people have disabilities or are experiencing high levels of stress may warrant alternative approaches, including ways to confirm identity when individuals do not have a driver licence.

Alternative approaches may include:

- putting processes in place to identify situations where it is acceptable to provide no, limited or alternative kinds of personal information
- enabling people to agree to some purposes their personal information can be used for, but not others
- enabling people to provide summary information if detailed information is particularly sensitive
- enabling people to provide information anonymously if the purposes of collection can accommodate this.

Find more information about offering choices to certain groups of service users in the Purpose Matters Guideline.

Purpose Matters Guideline: Assess purpose and only collect what is needed

Things to consider

- If you were asked, could you provide a clear explanation about why it is not feasible to offer people a choice about the collection of their personal information?
- Do you need any help to make decisions on these issues and, if so, who can help? Can subject matter experts or service providers or client representatives help?

Collect in a lawful and fair manner

Agencies need to ensure their actions are fair and reasonable when they collect people's information.

Collecting information in a lawful manner

While the Data Protection and Use Policy (DPUP) focuses on respect, trust and transparency, when it comes to the actual collection of personal information, the Privacy Act 2020's information privacy principle 4 (IPP4) — Manner of collection, requires agencies to collect the information by means that are lawful, fair and do not intrude to an unreasonable extent on the personal affairs of the people concerned.

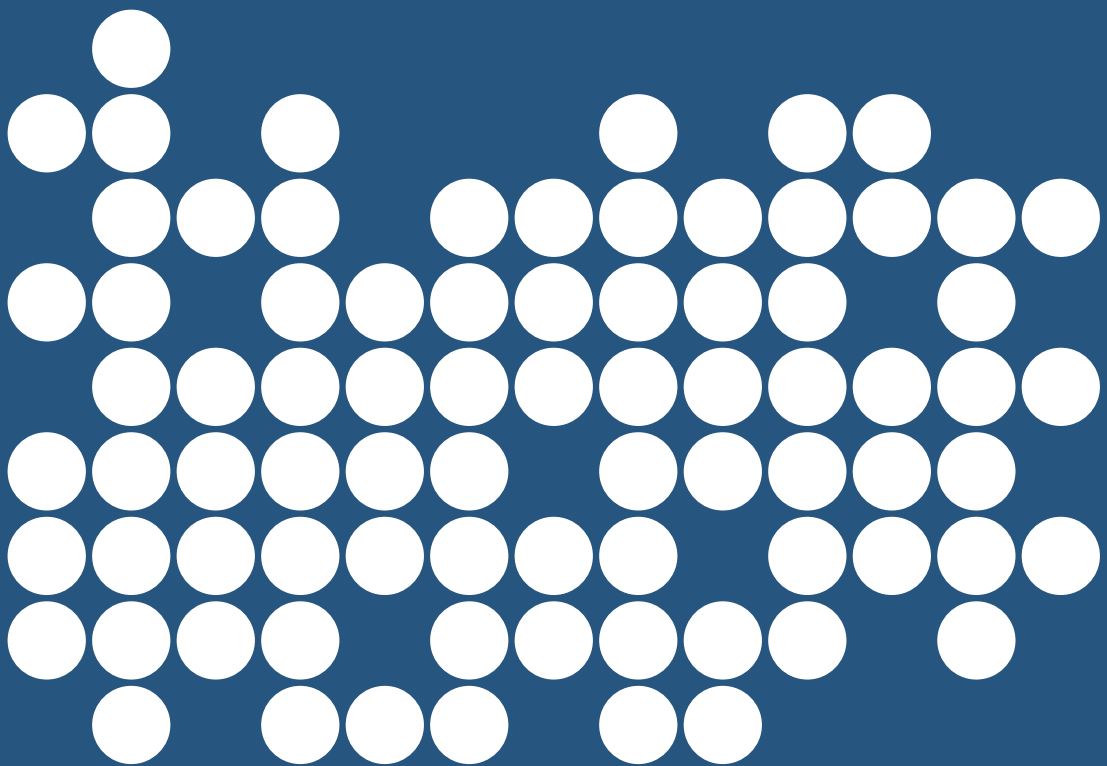
IPP4 also emphasises that particular care is needed when collecting personal information from children and young people.

IPP4: Manner of collection of personal information — Office of the Privacy Commissioner

Guideline

Access to Information

The importance of supporting people to understand what information is held about them and their right to access it.



Access to Information Guideline

Why DPUP has an Access to Information Guideline

When people are unsure about what information is recorded about them, or whether it is accurate or up to date, this can affect their trust or confidence in how it's used.

Access to Information's intent

This Data Protection and Use Policy (DPUP) Guideline recommends a proactive and pragmatic approach to ensuring that people understand and can exercise the options they have to:

- access their information
- request corrections to it
- in some cases, change it themselves.

This helps to address trust and confidence problems that can arise when people feel they have no practical or easy way to understand or control what's happening with their information.

It's recommended that agencies put these practices in place proactively and regularly. Use them to promote the rights people have and enable people to understand and exercise those rights at a time that works for them.

This Guideline supports the Privacy Act 2020 requirements for access and correction.

Information Privacy Principle 6: Access to personal information — Privacy Commissioner

Information Privacy Principle 7: Correction of personal information — Privacy Commissioner

Access to Information's key concepts

Take regular, proactive and practical steps to engage with people about what information is held about them, and to enable them to access it and ensure its accuracy.

This helps to build trust and confidence by:

- reducing people's concerns and frustrations
- supporting them with a sense of empowerment.

It can also help to ensure that agencies act on accurate information and people receive the most appropriate services for their situation.

Helping people understand their rights

People who use agency services may not understand what rights they have to:

- see the personal information that has been collected about them or is about them
- ask for that information to be corrected
- express a preference as to how they'd like to access their information.

Understanding these rights is important. Uncertainty may deter people from providing the information in the first place, or from accessing a service they need.

If an agency is proactive, and makes the process as easy as possible, service users are more:

- empowered
- confident that correct information will be used for the purpose it was collected for
- confident that agencies act on accurate information and the services they receive are the most appropriate for their situation.

Important reasons for this Guideline

- For many people, their information is an important part of their story and who they are. They want to feel confident their information is respected and treated with care. This includes enabling them to understand what information is held about them and why, and that such information is relevant and appropriate for the purpose it was collected for.
- Even where people broadly understand their rights, they may not understand how to exercise them or there may be a lack of practical opportunity to exercise them.
- When people are in a crisis or vulnerable situation, they may not initially be concerned about how they can access and request correction of their information. However, it is usually still important at the appropriate time to proactively ensure they understand and can exercise their rights to access and request corrections to their personal information.
- The difficulty people face in accessing their information can result in them having to repeatedly relive experiences. Sometimes retelling their story can be harmful for them. If they have already told their story to one agency and can get a copy to provide to another, it can save them from having to relive aspects of a traumatic experience.
- People sometimes assume that government agencies can share, access and exchange information about them without constraint. Enabling people to more readily understand what is known about them, and by which agencies, can reduce the sense of disempowerment this assumption causes.

Help people understand their rights

Help service users learn what rights they have with their personal information and how to use them.

Remind people about their rights

The Data Protection and Use Policy (DPUP) Transparency and Choice Guideline describes what agencies should tell service users when collecting their information, including their rights in relation to information held about them.

These can be summarised as the right to:

- understand what personal information is collected and stored
- access that information
- request correction of that information, bearing in mind the purposes for which it may be used.

Transparency and Choice Guideline

Accessing and correcting personal information

The Access to Information Guideline focuses on helping people to understand what personal information is held about them, to access it, to request correction of it and, where possible, to correct it themselves.

A range of factors can affect people's understanding of their rights, or their motivation to exercise them. For example:

- people will not always think about their information being collected or held when they initially seek help — they may be stressed in some manner and more focused on getting the help they need
- over time, more information about them may be gathered or created without their knowledge, such as information lawfully obtained from other agencies or information that is recorded about them when they are not present (for example, case notes)
- people often engage with several agencies on related topics — over time they may become uncertain about which agencies hold what personal information, what the personal information covers and what those agencies are doing with their information.

Information collection can create concerns

It is important when recording information about a person to ensure that it is accurate, clear and well-written, both as a matter of respect and because the person can request access to, and view, what has been written about them.

It is especially important to make sure that staff and other people's comments are carefully weighed, respectful and professional.

Agencies cannot refuse a person's request for personal information merely because the information was poorly written or expressed with insufficient care. However, an organisation can withhold personal information from a requester if the information is evaluative material.

Evaluative material — Office of the Privacy Commissioner

People may eventually have concerns about:

- where their sensitive information is held
- if any of their information is out of date or could be misunderstood
- if their information may not be helpful in terms of the services they need.

In addition, sometimes people become concerned about how their sensitive information is recorded. The act of recording a person's story can involve interpretation and adverse judgements that may include stigmatising, generalising or stereotyping.

If someone has these concerns and also does not know how to access or request corrections to their personal information, this can have a negative impact on their sense of wellbeing.

> It's important to proactively remind people of their rights from time to time. This gives people an opportunity to think about their information and exercise their rights if they want to. Making sure that people know what they can do and how helps them to feel more empowered in relation to their personal information.

Giving people access to their information

There are grounds to deny people access to their personal information, but these need to be considered on a case-by-case basis. They do not justify a general denial of a person's right to access their information.

The default approach is to grant people access to their personal information when requested unless one of the grounds to deny applies. For this reason, the existence of these grounds does not affect the importance of reminding people about their rights in relation to their personal information.

Note also that, if an agency refuses a person's request to access their personal information when no grounds for refusal applies, the Privacy Commissioner can require the agency to give the person access to their personal information.

When agencies can deny access to personal information

The grounds for an agency being able to say no to someone requesting access to their personal information are in Part 4 of the Privacy Act 2020. These recognise that other interests may be harmed if someone is allowed access to their personal information.

The most relevant grounds concern situations where disclosure would likely prejudice the:

- safe custody or rehabilitation of people convicted of an offence or detained in custody
- physical or mental health of an individual — if the agency is satisfied of this after, where practicable, consulting the individual's health practitioner
- maintenance of the law, including the prevention, investigation and detection of offences, and the right to a fair trial.

Disclosure may also:

- be likely to endanger either the safety of any individual or public health or public safety
- create a significant likelihood of someone being seriously harassed
- include information about another person who is the victim of an offence or alleged offence and the disclosure would mean they suffer significant distress, loss of dignity or injury to their feelings
- in the case of an individual under 16 years of age, be contrary to that individual's interests
- interfere with the privacy of others
- breach confidentiality or legal or professional privilege.

Part 4 of the Privacy Act 2020: Access to and correction of personal information — Parliamentary Counsel Office

> Legal professional privilege means protecting confidential communications between a lawyer and a client. If legal advice is protected by legal professional privilege, it may be protected from disclosure under the Official Information Act 1982 and the Privacy Act 2020, and does not need to be produced for inspection during discovery in legal proceedings. There are 2 categories of legal professional privilege.
>
> 1. 'Solicitor / client privilege' which applies to communications between a lawyer and a client, where the lawyer is acting in his or her professional capacity, the communication is intended to be confidential, and communication is for the purpose of obtaining legal advice
> 2. 'Litigation privilege' which applies to communications or information compiled for the dominant purpose of preparing for a proceeding or an apprehended proceeding.

An agency may also refuse a person's request to access their information if the information cannot be found, does not appear to exist or is not readily retrievable.

How to help people understand their rights

Agencies should consider these questions when helping service users learn what rights they have regarding their personal information, and how to exercise them.

- Will service users be asked how they want to be involved in managing their information?
- What needs to happen to enable service users to ask about their information from time to time and to feel comfortable and safe in doing that?
- How much support might they need to understand or exercise their rights?
- What steps can be taken to confirm that a person is aware of their rights?

Agencies should make the process easy by having:

- a process in place to deal with requests from an individual's representative
- operational practices that emphasise telling service users up front what is recorded and how they can access it — this may be in general terms or specific to the person in question.

Agencies need to be clear about limits.

- If there are limits, why do those limits exist, and are they lawful?
- What limits should there be on access, and how can service users be told about them up front?
- Is there anything that can reasonably be done to reduce or remove such limits safely to enable access to the information?

Exceptions to people only accessing personal information about themselves

Under the Privacy Act 2020, people can only request access to personal information about themselves. There are 2 main exceptions to this.

1. If an individual has authorised someone else to act as their agent or representative, that other person can make requests on behalf of the individual

2. If a child is too young to act on his or her own behalf or if a child has consented, a parent or guardian can request access to information for the child.

For the first situation, and as noted on the Office of the Privacy Commissioner's website, "[w]hen an access request is being made by a representative acting for an individual, the agency should ensure that the representative has the written authority of the individual to obtain the information. This can be done in a letter or email."

Find more information in section 57 of the Privacy Act 2020, and 'Can I request someone else's information?'

- Section 57 of the Privacy Act 2020 — Parliamentary Counsel Office
- Can I request someone else's information? — Office of the Privacy Commissioner

Help people to ask for their information

The Data Protection and Use Policy (DPUP) recommends making people feel confident about requesting access to their personal information.

Provide assistance

Service users may need to engage with a range of agencies who hold information about them. They may feel overwhelmed asking for their information or intimidated by the process. Sometimes people are simply too shy to ask.

Disability, culture, language or literacy may also prevent people from feeling comfortable asking to see their information, and can also result in general concerns about where their information is and which agencies have access to it.

It's important to note that the Privacy Act 2020 requires agencies to "provide reasonable assistance" to people who wish to request access to their personal information or request correction of their personal information.

Practical and proactive ways to help

- Offer the information about rights, without being asked for it, in a safe and comfortable way that supports the service user's ability to absorb and understand the information being provided.
- Check with service users on a regular basis to see if they would like to update their information, or if their circumstances have changed.
- Help people to use the Privacy Commissioner's AboutMe tool
- Offer to act as the person's agent or representative (where the person wants to request their personal information from another agency) and make appropriate requests on their behalf.
- Offer pre-prepared summaries listing which agencies will hold what kinds of information. This can help lessen concerns about agencies knowing things they would not ordinarily know, and/or focusing the conversation on the agency or agencies the person is most interested in

Make it easy to access and request corrections to information

Help service users to exercise their rights to see their personal information and request corrections to it.

How people can access information in person

Service users' personal information will be held either by:

- your agency for your agency's purposes or collected on behalf of another agency
- another agency.

If your agency holds the information

- Consider sharing your screen, showing people what's recorded about them, and asking them to identify any inaccuracies or voice any concerns they may have about that information.

- Provide printouts of your screen, or other pre-prepared reports your information and communications technology (ICT) system may offer, or allow them to take a photo if their phone has a camera. Ask them to highlight any areas they might wish to change.
- Email a screenshot to them, taking care to double-check email addresses, making sure they want to receive this information by email.
- Provide photocopies of relevant information.
- Supply the information in an accessible format that is appropriate to the needs of the person, such as for children, people with low literacy levels, sight-disabled people and those with English as a second language. What timing, language, format, visuals, flowcharts, pictures or other things could be helpful?
- Talk through the information to help with the person's understanding.
- Use a support person who can speak the person's first language to translate for them.

If another agency holds the information

- If a person asks your agency for their information but you believe another agency holds it, the Privacy Act 2020 requires your agency to transfer the request to the other agency promptly, within 10 working days, and to inform the person you've done so.
- Offer to help them fill out the Privacy Commissioner's AboutMe form or connect them to the other agency to help them ask directly.
- Fill out the AboutMe form on their behalf and act as their representative if, for example, they share an email address with a spouse or partner and would rather the information is kept private.
- If you have established relationships at an operational level with the agencies in question, contact them and ask on behalf of the service user, or with the service user present.
- Consider establishing a protocol with other agencies about access which will make it easier and more convenient for agencies and service users.

AboutMe — Office of the Privacy Commissioner

Help other organisations act on behalf of service users

Your agency may hold information that is useful and relevant for a non-governmental organisation (NGO) or other organisation to provide effective support for service users.

Service users may not remember or wish to recount relevant information when seeking a service. Instead, they may want the NGO providing the service to act as their representative and request the relevant information from the appropriate agencies.

Examples include:

- confirming details of benefits and entitlements
- information about health or wellbeing
- information about a person's overall situation that they may prefer not to repeat, given that doing so repeatedly can have negative impacts on their wellbeing.

> Having an NGO acting as their representative can reduce stress for the person seeking support, improve timeliness and the quality of the service they receive.
>
> It is also efficient for the agencies that are asked for an individual's personal information, as it provides clarity about what is needed and establishes channels and processes on how to best meet these requests.

Establish channels

To make it easier for people to access their information through others, agencies can:

- identify the organisations and types of services where it's practical and makes sense to act on behalf of service users — noting that expectations of volume and timeliness that are mutually agreeable will have to be worked through
- establish local or regional relationships between agency staff providing the information and the organisation acting as the service user's representative
- agree on appropriate processes (such as signed permission forms) to allow information to flow for lawful and agreed purposes when service users wish to access and check their records and want others to act as their agent or representative
- agree on who is the appropriate agency contact, how to contact them and what their responsibilities are, and identify who can do the work
- understand what information is typically useful and how it can be readily retrieved
- determine response times that can be reasonably achieved for typical requests, and agreed criteria for when a request is urgent
- have support in place when needed for urgent cases — for example, a mobile or direct dial number to call.

When establishing such channels, agencies may need to clarify general expectations about how people's information will be managed, who can see it, and so on, including aligning with relevant advice in the Data Protection and Use Policy (DPUP) itself.

Using digital or other channels

When deciding to deliver your service digitally, consider the following.

- Digital access — service users may not always be able to access digital channels for a range of reasons, including language, technical confidence, access to technology, time or disability. Knowing that digital channels exist, but are not accessible, can be frustrating. Consider making it easy for service providers or others to be a representative for service users, or to complement digital channels with suitable alternatives.
- Setting up access to digital channels — the most immediate hurdle for people may be understanding what digital channels exist, what they do and how to access them. Consider enabling providers to help service users establish access to these channels.

Provide access to a person's information in the form they prefer

The Privacy Act 2020 states that, where a person's requested personal information is contained in a document of any sort (which could be hard copy or electronic), the agency can make the information available by:

- allowing the person to look at the document
- giving the person a copy of the document
- giving the person an excerpt or summary of the contents
- telling the person what is in the document.

At the same time, the Privacy Act 2020 requires the agency to "make the information available in the way preferred by the requestor, unless doing that would be administratively burdensome, contrary to a legal duty over the document or prejudice a reason in the Act for denying a request".

Section 56 of the Privacy Act 2020 — Parliamentary Counsel Office

Things to consider to improve processes and systems

- How can service users be involved in creating records, for example, writing or reviewing case notes or filling out forms?

- For larger agencies, can technology plans include providing online portals such as myMSD and ManageMyHealth to allow people to access and update some information?
- Can processes or practices help service users avoid having to make formal requests for their personal information. For example, can your agency automatically provide copies of core information such as referrals, assessments and forms?
- Does your agency have simple, well-understood business practices for staff to retrieve and provide information in response to Privacy Act 2020 requests?
- What are simple ways for service users to ask for changes or corrections, for example, in similar ways to the AboutMe tool on the Office of Privacy Commissioner's website?
- How can service users' ideas and suggestions be included in regular planning processes to help define simple and efficient processes for them to access their information?
- Does your agency have simple and clear processes for service users to talk about their concerns or make a complaint?

MyMSD — Ministry of Social Development

ManageMyHealth

AboutMe — Office of the Privacy Commissioner

Only give people their own information

When helping people to access their personal information, it's important to check they're only accessing their own information and it does not contain or refer to other people's personal information. Allowing someone to view another person's information could breach that other person's privacy.

If someone requests personal information that is combined with information relating to others, it may be necessary to separate or redact the other information before granting access.

Acting as an agent or representative

The Data Protection and Use Policy (DPUP) stresses the importance of enabling people to use their rights. However, sometimes people may wish to ask someone else to act for them.

Giving permission to act as an agent

The service user can give someone permission to act as an agent or representative in the form of either:

- a letter
- a signed form
- an email.

Reasons for doing this might be due to a person's language ability, their culture, disabilities, whānau-based considerations or a range of other practical issues.

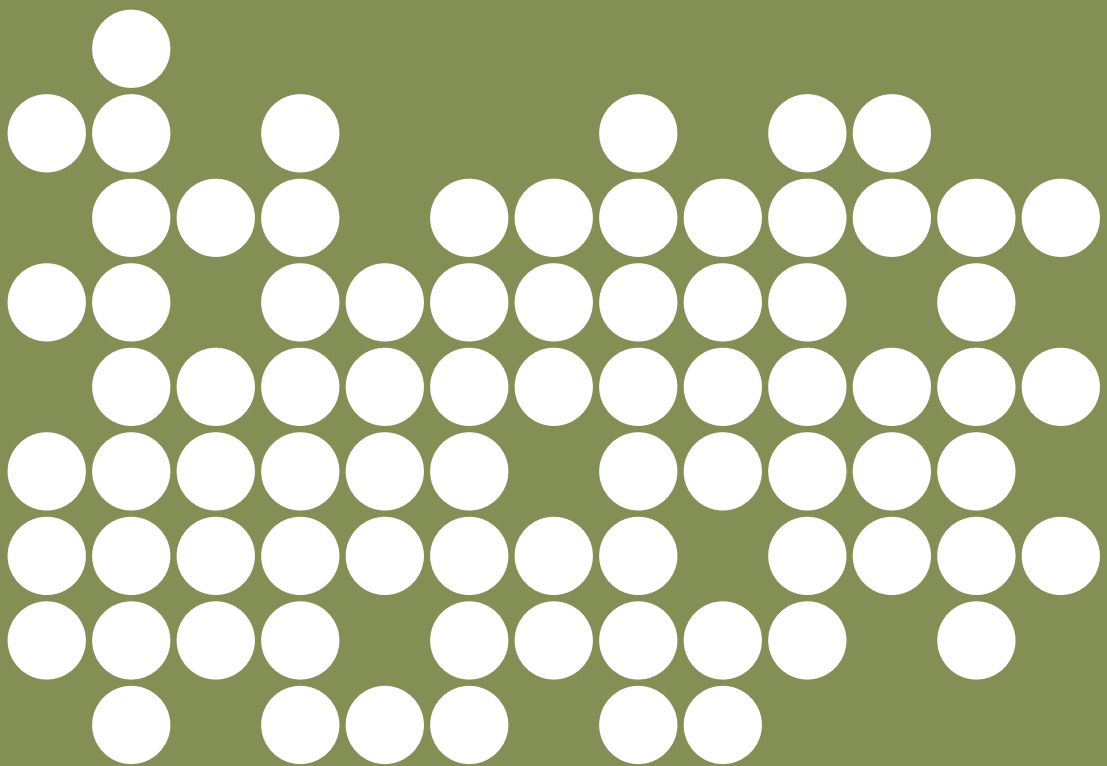
Further information is on the Privacy Commissioner's website.

Can I request someone else's information? — Office of the Privacy Commissioner

Guideline

Sharing Value

The importance of being inclusive and sharing insights.



Sharing Value Guideline

Why DPUP has a Sharing Value Guideline

It's important agencies develop and share information and insights with others in an inclusive, useful, respectful and valuable way.

Sharing Value's intent

This Data Protection and Use Policy (DPUP) Guideline recommends explicit collaborative actions between people and communities who share an interest in development or use of insights to:

- identify what the most useful information would be to support the development of the desired insights, including qualitative and interpretative information to help give context to quantitative information
- identify people and agencies with relevant interests and experiences to contribute to the work and use the relevant insights
- share the insights with those identified.

This Guideline's recommended actions are:

- about sharing insights as well as developing them
- common to many codes of practice as opposed to legal requirements.

Sharing Value's key concepts

Agencies can benefit from greater sharing of non-identifying insights derived from information collected from and about people. Such sharing can help improve services to these people and help their own agencies. This is best achieved by taking a collaborative approach.

Throughout the process of developing insights, it's important to involve those who have rich knowledge of the circumstances of the people information is collected from, even if this information will only be used in a non-personal form. This is the Value Loop.

This helps to ensure a good understanding of:

- the value of the insights that may be derived from this information
- the purposes of collection or use (see Purpose Matters Guideline)
- the specific type of information that would best suit those purposes
- how to gather that type of information in the most efficient and respectful way
- how to communicate the purposes and value to those the information is collected from
- any risks and downsides that may outweigh the potential value of collecting and using this information to develop insights.

Sharing Value: The Value Loop

Purpose Matters Guideline

Collaborating delivers value

A collaborative approach involves exploring:

- what the objectives of collecting and analysing information are, before those activities are carried out
- what insights will be most helpful to people and agencies working on related outcomes.

This approach aims to deliver value to all participants.

Important reasons for this Guideline

Service providers are often required to share information they collect with other agencies for accountability, research and analysis, and planning purposes.

Many people, such as decision-makers, government, non-governmental organisations, communities and service users, are likely to benefit from sharing insights derived from information collected from or about people. Such insights are valuable for supporting robust decision-making and better service delivery, which support positive outcomes.

Service providers and users want to be involved at the start of the information collection process and throughout the process of developing insights based on that information. This is so they can contribute their perspectives, expertise and suggestions, and have opportunities to understand, access and apply those insights.

Understanding this Guideline's terminology

- Insights — non-personal information, including data and data sets, analysis, qualitative or quantitative information, statistics, research, reports or studies, that may support improved decision making.
- Non-personal information — information that does not identify individual people.
- Sensitive information — information that could be misunderstood or misused, resulting in harm or embarrassment to a group or community.

DPUP terminology

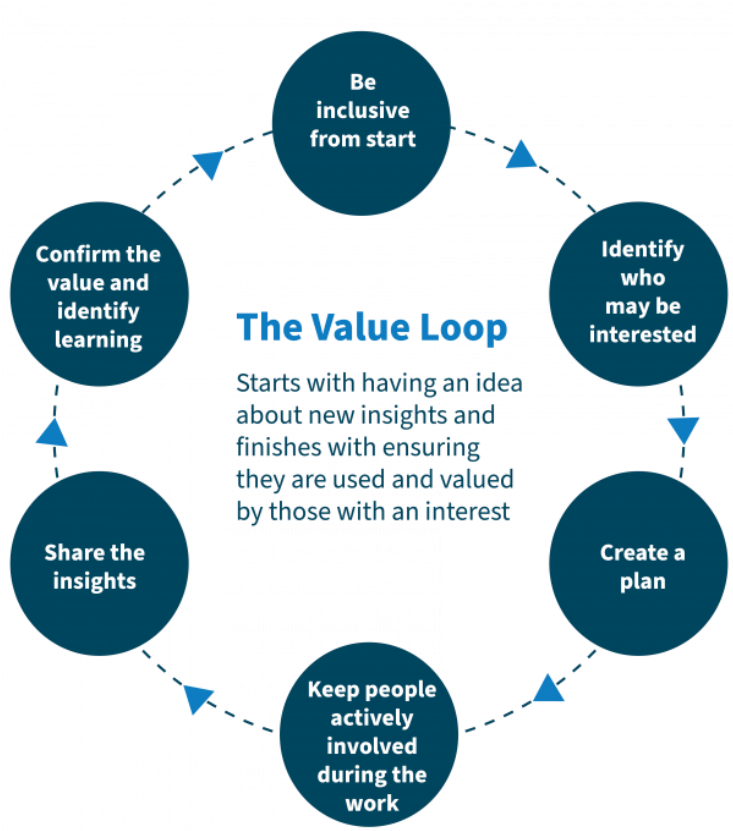
The Value Loop

Follow the Data Protection and Use Policy (DPUP) Value Loop when working collaboratively on new insights to develop and share the valuable results.

Understanding each step of the Value Loop

Each section in this Guideline defines a step of the Value Loop and the important things to consider at each step.

Diagram 1: The Value Loop



Detailed description of the diagram

Six circles are set out in a loop and connected by a dotted line going in 1 direction. Each circle has a label: 'Be inclusive from the start', 'Identify who may be interested', 'Create a plan', 'Keep people actively involved during the work', 'Share the insights', 'Confirm the value and identify the learning'. In the middle of the loop is the text: "The Value Loop — Starts with having an idea about new insights and finishes with ensuring they they are used and valued by those with an interest."

Overall objectives of the approach

Agencies need to make sure work on new insights include the right idea, right people, right information and the right use.

- Right idea: ensure the work is informed by a good understanding of the topic and is respectful of the people whose information is involved.
- Right people: ensure the people involved have interests aligned to the He Tāngata Principle — that is, they wish to improve the wellbeing of people or communities. For example, people working in and serving their communities.
- Right information: ensure that the right data is used or collected. The right data is relevant to the idea and may include both qualitative and quantitative data. Qualitative context can add significant understanding to the insights derived from quantitative data.
- Right use: ensure the value of the work is maximised through not only how it is done but also who can apply it in their own work to achieve better outcomes for people.

He Tāngata Principle

Things to consider

Agencies need to consider:

- if there is any risk that a person could be identified from the seemingly non-personal insights that might be shared. This can be particularly important when dealing with small population or sample sizes or where insights relate to something that affects only a small number of people, for example, a rare disease or disability.
- how this work will enhance the mana of the people the insights are about. For example, is there a development focus rather than a deficit focus in the insights being developed that considers the strengths and wellbeing of the people represented by the data rather than disadvantages and disparity?

Additional questions to ask:

- Will the community support the use of the data in this way?
- How can the work ensure no one is harmed or exposed, especially vulnerable people. For example, could insights be used to target, profile or prejudice people?
- What professional codes of conduct or ethical considerations are needed to guide this work?
- What contextual and cultural understanding is needed to fully understand the real experiences of the people behind the data so insights are relevant and accurate?
- Who will benefit from the insights?
- Who will contribute knowledge on the type of data that will be the most useful?

Be inclusive from the start

Include people with experience and involvement in the delivery and use of services from the start, and throughout it, to make the greatest impact on the eventual quality and value of the insights.

Improve the value of the insights

The value of the insights from analysing people's data or personal information depends on 2 things:

- having good information to work with
- being able to improve outcomes because the insights are relevant.

The Data Protection and Use Policy (DPUP) stresses the importance of an inclusive approach. Agencies can ensure the quality and value of the insights by including people with the right experience and involvement in the delivery and use of services from the beginning of the work.

There are several reasons to do this, in addition to improving the relevance, usefulness and value of the insights.

- It will help build agencies' capacity and capability in working with data. This increases collective ability to use insights to improve outcomes and helps build trust and confidence through an inclusive approach that recognises shared outcomes.
- It ensures the approach is informed by knowledge about the availability and quality of information, and what is involved in collecting the information.
- It can help reduce the effort that may be involved in collecting information. For example, similar information may already be collected for similar purposes and can be lawfully used or shared.

Identify who could be involved

The Data Protection and Use Policy (DPUP) recommends agencies should identify the people whose experiences and skills will help improve the value and quality of insights from the data.

Using different experiences to contribute to the result

If your agency is collecting or using personal or non-personal information for something other than directly working with a service user, consider who else should be involved.

It's important to identify and talk to people and other agencies with different areas of experience at each stage of the work:

- Service users — they provide the information and are the intended beneficiaries of improved outcomes. They can contribute to the approach and provide their perspectives on the best ways of sharing insights from the information collected from them.
- Frontline service delivery workers — they are involved in the original collection of information, even when it is ultimately used in a non-personal form.
- Communities — other agencies may be involved in providing similar services or with similar service users. They can influence the approach to developing the best insights.
- People involved with contracting, funding or partnering — they manage, monitor or account for the performance of funded programmes. These might include government agencies, philanthropic groups or community trusts.
- People involved in policy, analysis or research — these people may work in agencies working on related or similar insights. They can collaborate to reduce overall effort and increase overall value.
- Cultural experts — individuals with expertise in using data in a culturally appropriate manner. They can assist with the development or review of insights, taking into consideration the cultural context.

Things to consider

- Who should, could or must be involved given the nature of the work?

- If the potential insights may be useful to Māori or iwi groups, how might they be involved?
- If insights may be useful to other groups with specific interests, such as Pacific peoples or disabled people, are they involved?
- What processes are in place to involve service users' and communities' points of view, as well as non-governmental organisation and service provider input?

Create a plan

Create a plan for working together to proactively develop and share insights with people, communities and agencies who have an identified and legitimate interest.

Evaluate, consider and identify

Incorporate creating a plan into your agency's standard planning processes. Doing this at the start informs the approach and is critical to its success. Use this planning stage to:

- evaluate the intention of the work with respect to each of the Data Protection and Use Policy (DPUP) Principles
- consider any ethical concerns and relevant professional codes of practice
- identify and assess any risks or opportunities.

Things to consider

Agencies need to think about:

- Who could help with this planning step?
- When is the best time to discuss this? For example, when setting up a contract between funder and service provider, initiating a research activity, or during regular planning processes (yearly, quarterly) that can include a focus on existing collections of data and insights.
- Are there any legal requirements to share or, alternatively, obligations to keep some information confidential? What impact will that have?
- How can the outcomes of the work best be shared with service users, whānau, communities and service providers who have a legitimate interest?
- What kind of support might people need to understand or apply the outputs of the work? If there are different audiences with different needs, does the work address those?

In relation to data and information, agencies should think about:

- What data is needed to derive or inform the insights?
- What understanding of the cultural context of the data is needed?
- Does it have existing collections (of data or insights) that other agencies, involved in related outcomes, may be able to apply in their work?
- Is it possible to use existing collections to reduce further collection or overlapping activity?

Keep people actively involved during the work

The Data Protection and Use Policy (DPUP) recommends an inclusive approach. Maintain interest in the insights by giving updates, inviting feedback, collaborating and recognising people's contributions.

What involvement might look like

Ongoing involvement in analysing the data and providing insights may include:

- seeking regular feedback from people identified at the outset
- seeking more formal review of insights in draft form, for example from an advisory group

- day-to-day involvement from other agencies to develop the insights
  periodic secondments or structured collaborative projects.

Things to consider

- How can the effort and cost of involving others be recognised or shared?
- As the work is carried out, what's the best way to monitor that the developing insights are valuable and usable to others?
- If people are interested but only wish to be kept informed, how might that work?
- If others are working on related ideas, are there opportunities to collaborate and reduce overall effort or enhance overall value?
- If there will be effort involved in collecting the information, are there ways to minimise this or to recognise the cost of doing so?

Share the insights

Think about who might benefit from the insights, what they might need and how they will have access.

Consider the approach

Think about the nature of the insights and talk to those who may be interested in them. Get their views about what approach makes sense to them as well as to your agency.

Even if insights are sensitive in nature, it may still be very useful to share them in a lawful and appropriate way with people who can apply them for better outcomes for service users.

To ensure the value of the insights is realised, agencies that own the data or insights should always plan to share them. If they do not want to share the insights more broadly then the agency should explain why — this may be for legal, safety, cultural or other reasons.

Having access

These groups range from having less access to results and the results being less open through to having more access to results and the results being more open.

	Less access	More accesss	Most accesss
Who will have access?	Your team or agency	People directly involved	Broader stakeholders
What will they have access to?	Final results (PDF or Word version)	Data tables	Structured data
How will they have access?	In person with no 'takeaways' (for example, presentation)	Closed access	Wider access

> **Note**
>
> If the work is not sensitive and may have broad public interest, it may be simpler and more valuable to use an 'open data' approach. You can find more information on how to do this on Data.govt.nz.

In this context, to ensure the insights can be fully used without copyright-related concerns, government agencies can license copyright works containing the insights under a Creative Commons licence in accordance with the New Zealand Government Open Access and Licensing framework (NZGOAL).

NZGOAL is all-of-government guidance for agencies to follow when releasing copyright works and non-copyright material for reuse by others. If an agency takes this approach, it should follow the NZGOAL Review and Release Process to ensure it has the legal rights required to license the copyright works and that it takes other legal considerations into account.

NZGOAL — Data.govt.nz

Things to consider

- If the information is non-personal, but still sensitive, how can access be controlled to limit misuse or misinterpretation? Alternatively, will interested agencies need additional support to limit or reduce these risks?
- How is privacy being protected? When sharing insights with others, take all reasonable steps to ensure people cannot be identified from those insights, either from the insights alone or in conjunction with other information. This can be particularly important when only a small number of people are affected by the subject matter of the information. For example, the small number of people affected by a particular disability or condition.
- If sensitive insights are being shared with specific audiences and / or there is a re-identification risk, consider whether contractual controls on use and / or re-identification is a good idea.
- Are there any limitations or bias in the data (for example, data gaps or quality issues) that need to be communicated with the insights?
- Can the methodology and the software code used to produce the insights also be shared, for openness and transparency?
- Are the insights being shared in line with the original plan? If not, why not?

Share results with those directly involved

Give the people or agencies who were involved in the insights an opportunity to understand the insights and to use them. This may be the service users themselves, agencies involved in the original collection or creation of data, and people directly involved in doing or reviewing the work.

There may be other parties who have an interest in the insights, but it's important for trust and integrity reasons — consider the Data Protection and Use Policy's (DPUP's) Mahitahitanga Principle — to ensure those directly involved in the work can see the results. It recognises their contribution and increases value through broader application.

Mahitahitanga Principle

Confirm the value and identify learnings

Understand how people use information and insights and feed this understanding into future work.

Check in and share insights

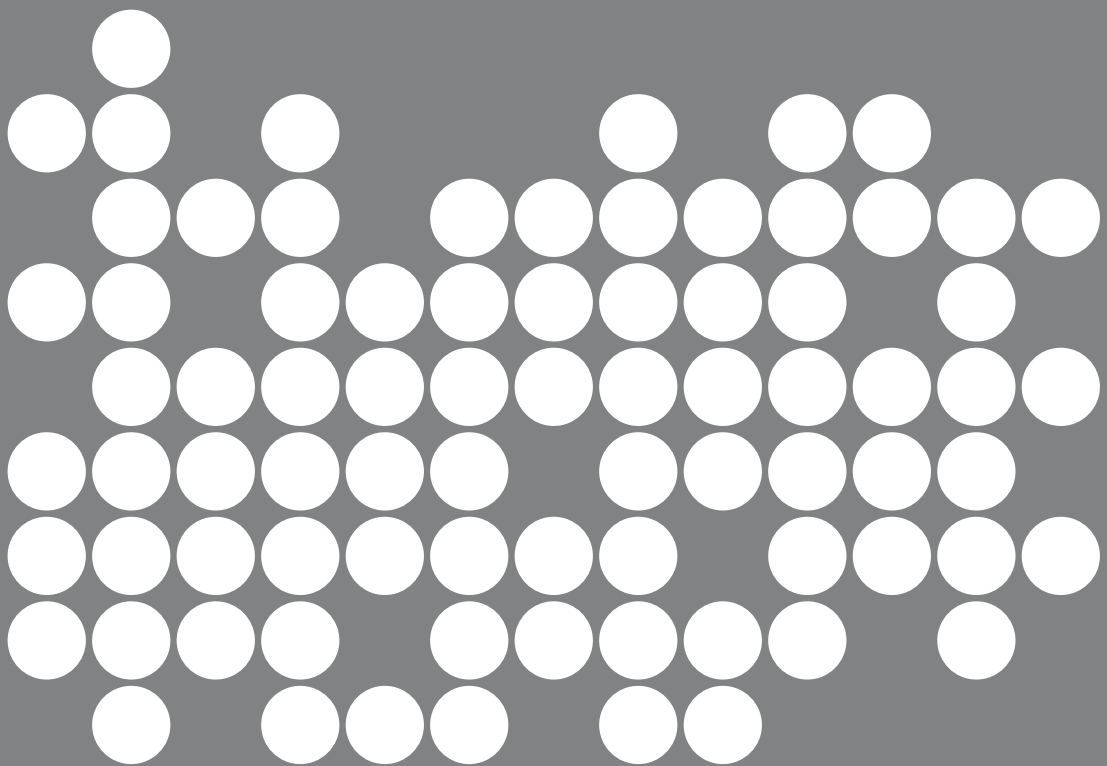
For most agencies, the work of developing and applying insights is ongoing. There are multiple 'value loops' in which agencies explore, consider and apply a growing understanding of how services can work better for people.

Regularly checking in with agencies and communities you've shared insights with will contribute to understanding what worked and what did not. These learnings can be used to inform the next cycle of thinking.

This process will enable a greater understanding of the value of insights and how they are being used to improve the wellbeing of people. The value of these outcomes can then be communicated back to people who provide their information.

See the Data Protection and Use Policy's (DPUP's) Transparency and Choice Guideline.molla

DPUP Terminology

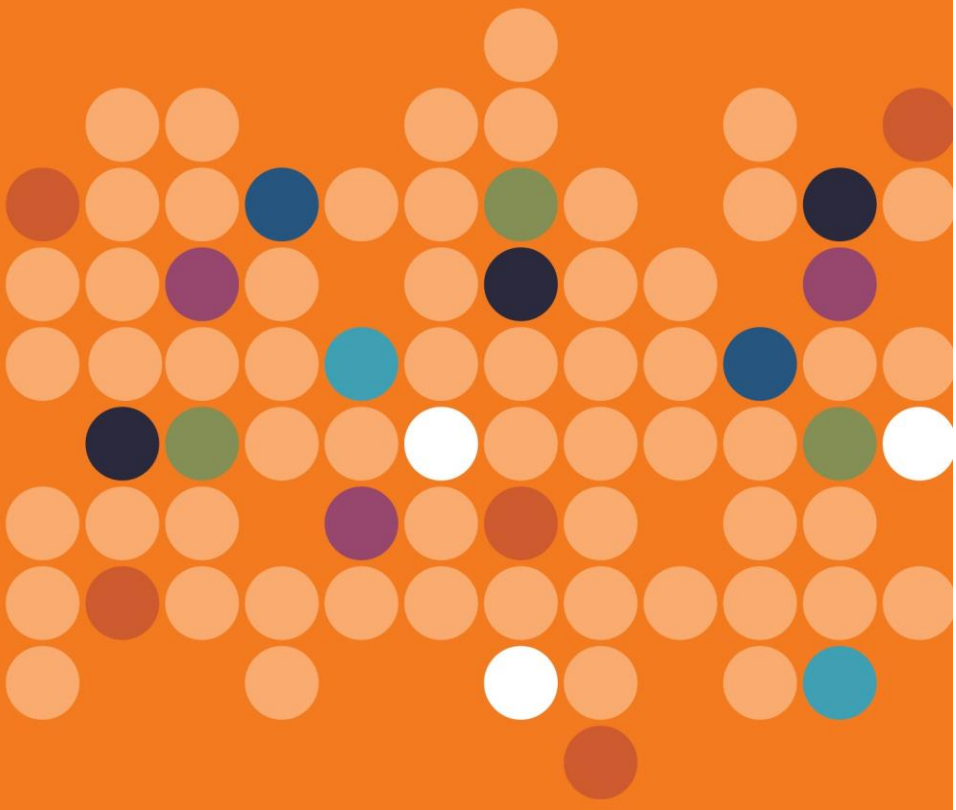


DPUP terminology

These key terms will help agencies understand the Data Protection and Use Policy (DPUP).

Term	Definition
Agency	Government agencies, non-governmental organisations (NGOs) and other providers of services.
Aggregated information	Can mean 2 different things, depending on how it's used. Aggregated information can be either: • summarising information by adding it together into statistics — for example, by counting the number of service users accessing a service over a period of time • larger collections of information produced by taking multiple sources of information and putting them all together — in other words, adding or 'aggregating' them together. Aggregated information can be personal (still contains people's identifiers in some form) or non-personal.
Consent vs. choice	Consent is given when a person voluntarily agrees to something based on a good understanding of the consequences. However, consent can have specific definitions in fields such as medicine, research and law. For this reason, DPUP uses a plainer word — choice — and focuses (in part) on the processes that help give people choices and enable them to act on those choices.
Data	Data can be defined in several ways, such as: • most simply as facts or information used to analyse or plan something, which traditionally has meant facts and figures • in the wider sense — as data sources and analytical approaches have become richer, data can take the form of numbers, stories, research, and analyses of these for greater understanding.
De-identified	Information that could identify an individual — like names, dates of birth and addresses — has been removed. Numbers that can be used to identify people, like IRD and National Health Index (NHI) numbers, are removed or encrypted (replaced with another number).
Insights	Non-personal information, including data and data sets, analysis, qualitative or quantitative information, statistics, research, reports or studies, that may support improved decision making.
IPP	Information privacy principle. Refers to any of the 13 key privacy principles in the Privacy Act 2020. The privacy principles: overview — Privacy Commissioner
Layered privacy statement	A privacy statement that a person can choose to view at a number of different levels, starting with a summary and offering greater detail for people who would like to see it.
NGO	Non-governmental organisation — refers to social sector organisations that support people facing challenges, such as welfare, health, education, justice, child wellbeing, housing, and disability support services. Examples include the Salvation Army, Barnardos, and Presbyterian Support. There are thousands of such organisations in New Zealand.
Non-personal information	Non-personal information is information that does not identify people and that cannot be used, even if combined with other information, to identify individual people.
OPC	The Office of the Privacy Commissioner. See their website to learn more about OPC, the Privacy Act 2020 and other aspects of privacy. Office of the Privacy Commissioner

Personal information	Information about identifiable individuals, which is the same meaning as in the Privacy Act 2020. Subpart 2 of the Privacy Act 2020 — Parliamentary Counsel Office It includes information relating to a death that is maintained by the Registrar-General under the Births, Death, Marriages, and Relationships Registration Act 1995 or any former Act (as defined in section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995).
Privacy statement	A privacy statement or privacy notice is an external statement addressed to anyone whose personal information is handled by an agency. It must be provided when an agency collects personal information from an individual. A privacy statement should include: • who the agency is and its contact information • a purpose statement, including: what personal information is collected, directly and indirectly, and how the agency will use the personal information • how the personal information is collected • who the agency will share the personal information with • if a law requires or authorises the collection of personal information, what the law is and whether collection is voluntary or mandatory • what the consequences are for the individual if any or all of the requested personal information is not provided • how the behaviour of website users is monitored • how individuals can access and correct their personal information.
Purpose statement	A purpose statement explains why you need to collect or use someone's information. The information in a purpose statement is often reused in: • privacy statements or notices • consent forms • privacy impact assessments • leaflets for service users • partnering agreements and contracts.
Research	Studying a topic, analysing a topic, exploring or researching.
Service delivery organisation	An agency responsible for direct delivery of services to service users. This includes agencies like the Ministry of Social Development (MSD) and the Accident Compensation Corporation (ACC), and organisations like the Salvation Army. It does not include agencies like the Social Wellbeing Agency that do not deliver services directly to service users.
Service provider	Another term for service delivery organisation.
Service user	A member of the public who applies for, receives or otherwise uses services delivered by service providers.
Social sector	The social sector is made up of government agencies, NGOs and other service providers to support New Zealanders' wellbeing across a range of areas — such as welfare, education, health, justice, child wellbeing, housing and disability support services.



SOCIAL WELLBEING AGENCY | TOI HAU TĀNGATA

Policy developed in collaboration with the social sector

New Zealand Government

Te Tari Taiwhenua
Internal Affairs