Privacy Commissioner
Te Mana Mātāpono Matatapu

The privacy principles & examples of risks and mitigations

Contents

In this section, we:

- provide a brief overview of each of the 13 privacy principles and what they mean in practice
- ask some key questions to help you assess the privacy impacts of your projects and potential risks
- give you some examples of mitigations to address identified privacy risks.

Using the privacy principles to follow the information lifecycle.

Each privacy principle deals with a different aspect of information management. Addressing each principle in turn will therefore help your organisation make sure it takes proper care of the information entrusted to it.

Each principle links with the others. For example:

- disclosure by one agency often involves collection by another agency
- unnecessary collection increases risks of unwarranted use or access
- poor security or unjustified retention of information creates risks of having inaccurate or outdated records.

On the other hand, use of privacy enhancing technology or techniques in one area can free you up in other areas.

For example, if you anonymise information, it will be harder to link information to individuals. You are therefore less likely to need to restrict access so tightly.

Types of mitigations and safeguards

Strategies to enhance privacy, or to reduce or mitigate privacy risks, can include:

- technical controls – such as access control mechanisms, encryption, and design changes
- operational controls – such as organisational policies or procedures, staff training, and oversight and accountability measures
- communication strategies – such as privacy notices, and consent-based collection processes.

Principle 1 – Collection of Information

Personal identifying information shall not be collected by any agency unless:

a) the information is collected for a lawful purpose connected with a function or activity of the agency; and

b) the collection of the information is necessary for that purpose.

What Principle 1 means in practice

Be focused – only collect personal information if you need to.

The most effective privacy safeguard is not to collect information in the first place if you don’t need it.

Good overall information management often stems from being clear about your purpose at the start. For instance, if your organisation isn’t clear about why it needs the information, it’s not going to know who needs to see it, or whether it’s being used properly, or how to explain to the individuals concerned what it’s doing with the information.

It’s not enough simply to say that you might need the information sometime, or that it’s easy to collect.

Key questions to ask (collection)

- What personal information is your organisation currently using? Will your proposal change what’s collected?
- Why are you currently collecting the information? Will your proposal change that purpose?
- What business process is enabled by having the information? Why is the information needed for that process?
- If you’re collecting new information, why do you need it?
- Are there specific laws or regulations allowing you to collect the information?
- Are there specific laws or regulations prohibiting you from collecting the information? (If so, the Privacy Act won’t help you because the other laws will override the Privacy Act. Change your proposal to fit with what the law allows. Or, if you’re an agency that can influence legislation, consider what options you have to initiate a law change).
- Is all the information a genuine “need to have” – or is it just a “nice to have”? What information can you do without?
- Will anonymous information do? If you don’t need to collect someone’s identity to deal with them, then don’t. It makes the privacy risks a lot lower.
- Are you collecting information as a proxy for a different or less specific piece of information? For example, if you’re proposing to collect people’s dates of birth, do you in fact only need their age or age band?

Common risk examples (collection)

- personal information is collected without a clear purpose or without clear legal authority.
- information collected is either unnecessary or excessive.
- decisions affecting the individual concerned may be made using irrelevant information.
- the purpose of collecting the information may be unclear, leading to possible misuse.
- the individual concerned may feel a loss of control over what information is collected.

Possible mitigations to better protect privacy (collection)

Establish the need for collection

- Clearly state your purpose for collecting the personal information.
- Limit the information you collect to what is truly necessary for that purpose.
- Consider whether you can use information that doesn’t identify the individual.

Limit unnecessary collection

- If you only need to verify identity, use accredited identity verification systems
- If you want to keep track of the numbers of visitors to a website, keep a count of visits, but don’t keep IP addresses.
- Use pseudonyms to distinguish people, instead of personal information that identifies them.
- Constrain your IT systems so that unnecessary information can’t be stored in databases.

- Ensure that application forms ask only for the necessary information, and only have room for that information.
- When using or installing security cameras or CCTV, use masking or pixilation technologies.
- Only record images where there is a potential security risk, and delete records promptly
- Clearly identify where optional information can be provided, and explain the implications of not providing that information (this links with principle 3)
- Provide opt-ins for additional services (and easy opt-outs for services that people no longer require).

Principle 2 – Source of Information

Where an agency collects personal information, the agency shall collect the information directly from the individual concerned, unless one of the listed exceptions applies.

What Principle 2 means in practice

Be direct – get it from the people concerned, wherever possible.

When you collect information about someone, you should get it from them directly wherever possible, and you should tell them why you need it and what it will be used for. Then what you do after that won't be a surprise to them. Also, it's often the people themselves who are best placed to provide accurate information.

You can collect information from another source if you believe that one of the exceptions to the principle applies. These include:

- if the individual concerned has authorised you to collect the information from someone else
- if the information is already publicly available
- if getting it from another source wouldn't prejudice the individual's interests
- if the information won't be used in a way that identifies the individual concerned (including where it will only be used for statistical, or research purposes and the individual won't be identified)
- if collecting it from another source is necessary to enforce the law, or for court proceedings, or to protect public revenue, or
- if collecting it from the individual concerned isn't reasonably practicable in the circumstances.

Key questions to ask

Defining the source of information

- Who will you collect the information from – directly from the person concerned or indirectly from a third party? If a third party, then who?
- If you're collecting it from a third party, why won't it work to get it directly from the individual?
- Will this differ from the way you already collect information? If so, how?
- Do you need to positively identify the individual concerned, to check it's the individual who's entitled to deal with you?

Common risk examples

- Individuals may not be aware that information is being collected, who will use it or what it's being used for. If they become aware only later, they may be surprised and upset.
- Collecting the information from a third party could perpetuate and compound any errors that are already in the data.
- Information may be out of date or irrelevant for the intended purposes if it's used outside the original context in which it was collected.
- Individuals won't be able to update their information if they don't know you have it.

Possible mitigations to enhance privacy

- Change your system to collect information directly from the individual, unless you have a good reason not to do so. It's much better customer service to let the individual know what's going on.
- If you're collecting information from a third party, make sure the individual that the information relates to knows you're going to do that, unless there's a good reason not to.
- Have a clear privacy statement saying where you get personal information from.
- Provide people with a way to see the information you hold about them (like a dashboard) and give them the opportunity to correct it if it's wrong.If you're getting only verbal consent, make sure you have a good system to record or document that consent.

Principle 3 – Collection of information from the individual

Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of:

a) the fact that the information is being collected; and
b) the purpose for which the information is being collected; and
c) the intended recipients of the information
d) the consequences (if any) for that individual if all or part of that information is not provided
e) the rights of access to, and correction of, personal information provided by these principles.

These steps shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

What Principle 3 means in practice:

Be open – tell people why you need it and what you'll do with it.

When you collect information from an individual, whether this is voluntary or compulsory, you should tell them what you need it for, and what you're going to do with it. If they don't have a choice about giving information to you, spell out what statutory provisions require them to do this, and any limits on how those provisions can apply.

As with principle 2, there are some exceptions that allow you to not spell out what you're doing – for instance because it:

- would frustrate the lawful purpose of collecting the information
- could prejudice a criminal investigation
- is not reasonably practicable in the circumstances.

Key questions to ask (collection from the individual)

- Are your privacy statements easy to understand and access? (bear in mind the device or format that people will be using to read it)
- Will you have to change your privacy statements because of the change that your project involves?
- Do individuals need to acknowledge that they understand what information is being collected?
- If any new or additional information is being collected, has the purpose been defined?
- If you're telling the individual they have to provide the information, do they genuinely have to provide it or are you just hoping they're happy to provide it?
- If you're not spelling out the matters listed in principle 3, will these matters be obvious to the individual? If they're not obvious, do you have a good reason for not telling people?

Common risk examples (collection from the individual)

- Privacy statements may not be easily accessible – for example, on a mobile device with a small screen, or for individuals for whom English is a second language.
- People often don't read privacy statements – if your organisation acts on the basis that the individual has knowingly consented, this could lead to clients losing trust in you.
- The individual's consent for collection may not be supported by a valid, clearly explained purpose.
- Individuals may be surprised by information being collected that wasn't required previously.
- If they're not given advance notice, individuals may feel a loss of control over their information.
- The individual may lose trust in dealing with your organisation, ultimately leading to a lack of engagement that may affect your ability to meet your objectives.

Possible mitigations to enhance privacy (collection from the individual)

- Make sure your privacy notice is in plain language. Provide brief, key information first, and put explanations and details later (for instance, provide a link that people can click on for more information).
- Allow people to opt in if that's feasible. If it isn't possible, make sure people can clearly opt out.
- Make it clear to the individual whether providing the information is compulsory or voluntary. If it's voluntary, explain why it would be beneficial to have the information.
- Ensure your privacy notices are consistent and accessible in hard-copy and online.
- Review your consent process to ensure that consent will be informed, current and specific, and given by someone with the capacity to provide consent (e.g. a parent).
- Provide a privacy notice after collecting the information if it's not practicable to do so in advance.
- Publish privacy notices in formats and languages appropriate for the target group.
- Design privacy notices for use with adaptive technology such as screen readers.
- Update your application forms and enrolment forms to explain clearly why information is needed.
- When collecting data electronically, use the technology to your advantage (for example, highlighting updates to privacy policies, using different levels of web pages for different layers of details).
- Require positive confirmation for actions by the organisation that could lead to adverse effects for the individual.
- Change preference formats to yes/no options, rather than ambiguous check boxes.
- Set privacy-protective options as the default wherever possible.
- Use appropriate signage to ensure people are aware if CCTV surveillance is taking place.
- Publish PIA reports so individuals know how their personal information will be managed.

Principle 4 – Manner of collection

Personal information shall not be collected by an agency:

a) by unlawful means; or

b) by means that, in the circumstances of the case (particularly where personal information is being collected from children or young persons),

i. are unfair; or

ii. intrude to an unreasonable extent upon the personal affairs of the individual concerned.

What Principle 4 means in practice

Be considerate, be fair and don't be unreasonably intrusive.

Even where you're required to collect information, you often will have choices about how you collect it. Design your system so you collect information by the least intrusive method available, bearing in mind the purpose you're trying to fulfil.

Extra care should be taken when collecting personal information from tamariki (children) or rangatahi (young people).

Key questions to ask (manner of collection)

- How are you collecting the personal information?
- Is the collection overt or covert? If it's covert, why? (Covert collection is less likely to be fair – there needs to be a clear justification)
- Do you have to collect information that way, or do you have other options that would be as efficient or that might bring different benefits?
- Is the individual likely to be upset by the fact you're collecting in this way?
- Are you legally required to collect information in this way?
- Are you collecting information from children or young people? What additional steps might you need to take to ensure you are doing so in a fair way?

Common risk examples (manner of collection)

- Collection methods may be unjustifiably intrusive (for example, if biometric information is collected.
- Unnecessarily, or drug testing is conducted unjustifiably, or audio or video recording or location-tracking technology is used without adequate reason).
- Recording equipment is badly located or improperly adjusted, resulting in an over-collection of information, or an unjustified intrusion.
- The physical and mental health and well-being of an individual could be damaged through breach of trust and a sense of loss of control over the use of their information.
- Information is collected unfairly by using duress, coercion, or deception.
- Information is collected from individuals who believe mistakenly that they have to provide it because the statutory limits haven't been clearly explained to them.
- Information is collected from children or young people who don't understand why it is being collected.
- No steps are taken to address the power imbalance between the agency collecting the information and the children or young people they are collecting it from.

Possible mitigations to enhance privacy (manner of collection)

- Use masking technology to avoid having CCTV overlooking neighbouring properties.
- Think carefully about the different options available for collecting the information and choose the least intrusive option that still achieves the purpose.
- Check that every item of information on your form or your website log-in is necessary.
- Test whether people will really see and understand your privacy notices.
- If providing the information is optional, say so.
- Make sure you're not going to collect additional information by accident (such as audio material as well as video, where only the video is needed for the purpose).
- Don't drug test employees if they're not working in safety-sensitive positions.
- Think about whether you to need to get consent from family/whanau to collect personal information from their tamariki or rangatahi.

Principle 5 – Storage and security of information

An agency that holds personal information shall ensure:

a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against
   i. loss; and
   ii. access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
   iii. other misuse; and

b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

What Principle 5 means in practice

Take care – keep it safe.

You need to ensure that personal information is protected against misuse, loss or theft. Security is going to be relevant to you whether you're maintaining or upgrading an existing database of client information, moving information into a new application or other system, or developing a new business process or access model that changes how personal information is used or who has access to information.

There are some additional things to consider if you're using a third party to support IT systems or business processes and giving them access to the system that holds the information. You'll need to check that the third party has reasonable security safeguards in place.

Key questions to ask (storage and security)

- What personal information will be stored by the organisation and how will that change?
- What format will the personal information be stored in (paper, or electronic), where will it be stored, and who will be responsible for its safe-keeping?
- What security and access controls will protect personal information against misuse, accidental loss, unauthorised use or disclosure – whether in transit or when the information is stored and used?
- Who can access the information now, and how will that change?
- Are you using a different contractor from before?
- When did you last look at your security controls? Do they need updating?
- Do contracts with third-party providers include appropriate privacy clauses and safeguards? Will you know if something goes wrong when the information is in the third party's hands? Who from their staff will be able to see the information, and are they trained to handle it well?
- What policies, standards and procedures relating to storage will need to be considered (such as requirements for disposal; obligations to disclose to other agencies)?

Common risk examples (storage and security)

Electronic and technical security measures

- Failing to limit edit-access to data, or to limit or monitor access or enforce access controls, can lead to misuse or unauthorised disclosure.
- Devices in shared work areas, or portable devices, can provide for inappropriate access.
- Providing online log-in access to client records raises the risk of session crossovers, or automated scams.
- The system can't trace who has accessed a file – so you can't tell whether there are problems with unauthorised access.
- Unwarranted access to personal information may lead to identity theft.
- The organisation doesn't comply with basic standards and expectations for information security and records management.

Physical and operational security measures

- Staff are unaware of their obligations, leading to accidents, careless actions or mishandling of information, which in turn results in unauthorised disclosures.
- Co-located offices, shared workstations, uncontrolled building access and offices open to the public can pose a risk of unauthorised access to personal information.

- Failing to recognise the high-risk nature of information, including the need to implement a higher degree of security to protect particularly sensitive financial or health information.
- Failing to include contracted service providers in an agency's data-management strategy, elevating the risk of external breaches of data security where contracted service providers are located outside New Zealand giving rise to jurisdictional issues.
- Allowing workplace use of portable storage devices (such as USB sticks, mobile phones, personal laptops) without proper security protections.
- Using regular post to send highly sensitive personal information may raise the risks that it could be sent to the wrong address or go missing.
- Testing and training environments may expose personal information to risk.
- Hacking, system failures, data compromise or breaches result in unauthorised access.

Possible mitigations to enhance privacy (storage and security)

Electronic and technical security measures

- Limit the use of portable storage devices through operational policies and technical controls.
- Use registered post to send particularly sensitive information, rather than regular post.
- Use window envelopes to avoid mis-matching labelled envelopes and their intended contents for bulk mail-outs, but ensure that no information, beyond the name and address, is visible through the window.
- Ensure any remote access to your data, whether by staff or clients, is to encrypted data, or is unencrypted data that travels only via encrypted transmission.
- Use technologies such as CAPTCHA to differentiate between human and computer users of your site.
- Consider two-factor authentication rather than just username and password, and build-in a "time out" limit on access.
- Provide for degrees of anonymity (such as by using pseudonyms, anonymisers, or anonymous data credentials) to minimise the amount of data provided, allowing customers to reveal only so much personal information as is necessary in order to complete a transaction.
- Provide a degree of "unlinkability" (for example, by using multiple virtual identities and communication anonymisers) to hide real online identities (email address, IP address, and so on).
- Replace identifying details with non-traceable, disposable identities not readily associated with other identities used by the individual (for example, pseudonyms, one-time emails).
- Mitigate against loss or theft of sensitive information by protecting it in storage, in transit and in use with strong authentication.
- Encrypt confidential data when it is stored or relocated to data repositories or archival warehouses, providing for decryption keys based on data receivers' credentials.
- Keep processed data in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were originally collected.
- Ensure access and handling protocols define who has the authority and ability to add, amend or delete data and to assign, change or revoke access privileges.
- Provide in-house users with delay-send options and pop-up reminders to check attachments before sending to outside recipients and disable auto-complete for external emails.
- Embed technically feasible default privacy settings into the systems supporting the initiative.
- Use cryptographic tokens or credentials issued by organisations to allow individuals to anonymously prove statements about themselves and their relationships with public and private organisations.

Physical and operational security measures

- Ensure “sign-in” procedures don’t unnecessarily reveal information about previous visitors.
- Develop plain language usage policies to supplement your other data security measures.
- Ensure your projects include ongoing staff training that’s relevant to the jobs people do.
- Ensure physical security prevents unwarranted access to areas where sensitive data is stored.
- Ensure your records practices comply with recognised best-practice guidelines or standards.
- Ensure that particularly sensitive personal information, such as biometric information and health or financial records, attract the highest levels of security.
- Examine your data flows to identify any weak spots that need further security measures.
- Ensure your data security strategy is appropriate to the type of data stored.
- Ensure that service providers are contractually bound to comply with specific privacy safeguards.
- Conduct a threat and risk assessment of your database and network security.
- Engage someone to conduct an ethical hacking exercise to test system vulnerabilities.
- Use only dummy data in testing and training environments.
- Allocate a needs-based, unique identity to each authorised user.
- Take appropriate measures to identify and punish employee browsing.

Principle 6 – Access to information

Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled:

a) to obtain from the agency confirmation of whether the agency holds such personal information; and

b) to have access to that information.

What Principle 6 means in practice

Keep people informed – tell them what information you hold.

In most cases, people have a right to access the personal information you hold about them. That means you need a system that enables you to find information about people when they ask and provide it to them. There are some exceptions, though, and it's important to know what they are.

Records-management systems must consider the fact that individuals may wish to access the information an agency holds about them. Shoddy information-management practices are not an excuse. Most organisations don't have to hold on to information forever, but while you do have it you should be able to find it – wherever it is (onsite, in archives, offshore, in people's inboxes – or even in their heads).

The clock will be ticking too – you have to provide a decision about access as soon as reasonably practicable, and not more than 20 working days after the request comes in (unless you have a valid reason to extend this time limit). You also have to provide the information itself without undue delay.

Key questions to ask (access)

- How is personal information currently being stored and how will this change?
- What metadata is kept allowing personal information to be readily identified and located?
- Will all the information about an individual be in one place or clearly linked to ensure a complete record can be identified?
- If you get a request for the information, how would you respond and how long would it take you to decide about the request?
- Who is responsible for handling information requests? How will you make sure the request gets to them?
- If information is held in third-party storage (in the cloud for example) have you made sure you can get it back when you need it? Will it be in a format that you can use, and that you can easily supply to the requester?

Common risk examples (access)

- Changes to database structures affect the location and retrieval of information.
- Backup changes alter how information is retained and whether it can be readily identified and attributed.
- Individuals can't easily access their personal information.
- Lack of access to personal information increases the risk of poor-quality, outdated data.
- Access may be hampered if the data is held by contracted third-party service providers – there could be time delays to factor in.
- Information may be stored in a different format from the one that you can use now.
- Failure to file information properly leads to inefficiencies (for example, having to search through email inboxes rather than retrieving the information directly from the filing system).

Possible mitigations to enhance privacy (access)

- Make it easy for people to access their information by setting up a process for them that suits the way your organisation works.
- Make sure you keep accurate track of requests for personal information (whether they're verbal or written requests).
- Consider providing individuals with routine access to their personal information, or direct access – for example, through online accounts.
- Ensure that stored information is readily identifiable and retrievable.
- Ensure that contracts with external third-party service providers include provisions guaranteeing speedy retrieval of personal information when your organisation wants it.

- Increase the control that users have over their personal data by allowing them to look up past transactions using their personal information, including what data has been transferred or disclosed to third parties, when, to whom, and under what conditions.
- Inform users of their data access and correction rights, and who to contact if they want to request access.
- Have a standard process for people to use to demonstrate that they have authorisation to get information on someone else's behalf.

Principle 7 – Correction of information

Where an agency holds personal information, the individual concerned shall be entitled:

a) to request correction of the information; and
b) to request that there be attached to the information a statement of the correction sought but not made.

What Principle 7 means in practice

Make it right – let them correct it if you have got it wrong.

If you hold information about an individual that they think is wrong, they're entitled to ask you to correct it. If it really is wrong, it's in everyone's interests to get it right.

Sometimes, the person's opinion of what is right may differ from your own. In that case, you don't have to delete or correct the information. However, if the person wants you to, you have to add a statement of what the person thinks is correct to your file, in such a way that anyone reading it later will know what that person's view of the information is, as well as your own.

If you correct information, but you've already passed the original information on to another organisation, you should, if possible, notify the other organisation that the information has been changed.

Key questions to ask (correction)

- How do you accommodate individuals who believe that the information you hold is inaccurate?
- Does your system or process allow information to be modified if it's wrong?
- How do you verify the accuracy of information before you change it?
- How do you monitor changes to ensure they're authorised?
- If information can't be changed or appended, what mechanism is in place to attach a statement of correction?
- Will your system track who you've sent information to, so that you can let them know if the information was inaccurate and had to be changed?

Common risk examples (Correction)

- Poorly managed correction requests can lead to poor-quality data.
- Correction may be hampered if the data is held by contracted service providers.
- Failing to correct personal information that has been disclosed in the past can lead to inaccurate information, affecting the individual and the organisation's services.
- Computer systems aren't built to allow statements of correction to be added, or for a flag to signal that there is further information a decision-maker needs to consider.
- Poor quality information is passed to other agencies, compounding the errors and the problems for the individual.
- Information is duplicated in different parts of the organisation but corrected only in one.

Possible mitigations to enhance privacy (correction)

- Ensure there's a clearly defined process by which an individual can discuss or dispute the accuracy of the personal information you hold about them.
- Ensure you have policies setting out how your organisation can action routine or simple correction requests (such as a client's formally notified change of address), and who can determine more complex requests (for example, when a client disputes your decision on their eligibility for services).
- Design your system to allow a statement of correction to appear beside the original information – or at the least for the system to display a clear flag showing that there is other relevant information to consider.
- Ensure a record is kept of correction requests, and the decisions on those requests.
- If you have to keep the original information (for example because of statutory or record-keeping obligations), design your system to do so.
- Where services are contracted out, consider which organisation will have the most current and accurate data, and how any corrections will be communicated to the other organisation.

- Specify whether correction requests are to be mediated by your organisation or handled directly by the contracted service provider.
- Let users know about their access and correction rights, and ensure they know who to contact if they have a request.

Principle 8 – Accuracy of Information

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

What Principle 8 means in practice

Keep on the mark – ensure its correct and relevant before you use it.

Poor-quality information leads to poor decision-making, which in turn may lead to unfair and inappropriate practices and unwarranted adverse effects on the individuals concerned.

Poor data may also make it harder for agencies to perform their functions efficiently and effectively and meet their objectives. Inaccurate or outdated information can be particularly problematic, both for agencies and the individuals concerned, if agencies can't get in touch with individuals when they need to in order to verify their details and circumstances.

Key questions to ask (accuracy)

- What processes do you have in place to ensure the information you hold is attributed to the correct person (and not someone with a similar name or the same address)?
- What mechanisms are in place to ensure that information is accurate, complete, and up to date before it's used or disclosed?
- What opportunities are provided to individuals to routinely correct or update their personal information, or to verify its accuracy before it's used or disclosed?
- Is this information that's likely to change over time (such as address, marital status, financial or health status) or information that is static (birth name, date, or place of birth)?

Common risk examples (Accuracy)

- Poor-quality information may lead to decisions that impact negatively on individuals.
- Incomplete or incorrect information can lead to incorrectly informed decisions.
- Incomplete or inaccurate information may lead to financial or professional loss if used as a basis for decisions on whether an individual is eligible for a grant or benefit or has obligations.
- Information kept too long can be out of date.
- Information in misplaced files or that is positioned wrongly in databases can cause information to be attributed wrongly, while at the same time being dis-associated from the person concerned.
- Migrating paper records to a digital format by re-keying data risks introducing errors.
- Inaccurate data can increase the risk of inappropriate use and unwarranted disclosure.
- Updating personal information without creating and maintaining audit trails of the updates increases the risk of unauthorised changes going undetected.
- Failing to update personal information that has been disclosed in the past or that is held by contracted service providers can lead to poor data quality and inconsistent actions.

Possible mitigations to enhance privacy (accuracy)

- Regularly check the reliability of equipment used to collect, process or test information or samples to minimise errors and detect unauthorised changes.
- Before you take adverse action against someone based on the information, give them the opportunity to question or refute its accuracy.
- If information was collected some time ago, review your policies and practices to ensure it's still required for the purpose it was initially collected for and that your continued use of it is justified.
- Take care when engaging in data matching or cleansing
  - the data may already be out of date.
- Allow individuals to opt out easily for services they no longer require so you don't keep information on their current file longer than needed.

- Where information disclosed to another party is found to be inaccurate, let them know.
- Periodically assess the accuracy and currency of the information you hold.

Principle 9 – Deletion of information

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

What Principle 9 means in practice

Don't be a hoarder – get rid of it if you don't need it anymore.

Obviously, you can't destroy documents that must be retained under other laws (for instance, to comply with the Public Records Act or Tax Administration Act).

However, you need to make sure that any historical documents retained for those purposes are kept secure and can't be accessed by staff who don't need to see them. Consider whether, and when, the organisation should destroy any copies of documents that have been transferred elsewhere for permanent archiving. Also, consider de-identifying the information if it is to be retained for future business planning or research purposes.

Key questions to ask (deletion)

- How long do you need to keep the information for?
- Do you have a system saying when it's time to dispose of it, and how to dispose of it?
- How long have you already held the information, and if it's new, how long will you hold it?
- Is the information covered by the Public Records archiving requirements? If so, what protocols are you suggesting should be applied to protect the information once it's archived?
- Are there legislative requirements that mean you need to keep the information (for example, to comply with tax obligations)?
- Are there business reasons for keeping the information indefinitely (for example, to provide proof of a qualification from an educational institute)?
- Do you need to keep information with identifiers attached, or can you reduce it to anonymised or aggregated data and still get the job done?

Common risk examples (deletion)

- Keeping data longer than necessary increases the risk of a data security breach or unauthorised use or disclosure.
- Keeping information too long increases the risk it will be out of date, misleading and inaccurate.
- The careless or ineffective disposal of files may lead to unauthorised access or disclosure
- Destroying information when you still need it creates problems of its own – if you don't have a plan, you're likely to make mistakes.

Possible mitigations to enhance privacy (deletion)

- Have clear retention policies and disposal schedules, and monitor their use to ensure they can be updated as the need to keep information changes with time.
- Where you no longer need information for the purpose you collected it for, but you need to retain documents to comply with specific legislation (such as the Public Records Act or Tax Administration Act), add safeguards to remove it from view and prevent access except by properly authorised staff.
- Destroy transactional data when the transaction is complete and keep only metadata.
- Ensure personal information is disposed of promptly once the minimum retention period specified has expired unless you have a legitimate purpose for retaining it for longer.
- Design your database to include a facility to flag records for review or deletion when the minimum retention period expires.
- Ensure hard disks are entirely wiped or encrypted before disposing of computers. Use a shredder or secure disposal bins for disposing of paper records.
- Minimise the amount of information that needs to be disposed of by minimising the amount of information collected in the first place.

Principle 10 – Use of information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds, the specified exceptions apply.

What Principle 10 means in practice

Stick to the plan – only use it for the purpose you initially collected it for

Use information for the purpose you initially collected it for unless additional permissions and safeguards are in effect.

When information is going to be used for a different purpose that isn't directly related to the original one, you may sometimes need to notify the individuals in the same manner as if the information was new or additional information. There are exceptions – for instance, if the information is only being used for research or statistical purposes, and the individuals will not be identifiable in any material published at the end.

Other exceptions may also apply on a case-by-case basis: for instance where the individual concerned has authorised you to use the information for another purpose, where you took the information originally from a publicly available publication, or where it is necessary to enforce the law or for court proceedings, or to protect public revenue. You can also use information for a purpose other than your original one if you consider it's necessary to protect public health or safety or the life or health of the individual concerned or another individual.

Key questions to ask (Use)

- What personal information will be used and for what purposes?
- Is the purpose the information is to be used for directly related to the purpose for which it was collected initially? In other words, would the individual concerned expect that this was what you would do with it?
- Are there any controls or systems in place to restrict how information can be used?
- Are you using information for a new purpose. or is what you're doing within the scope of the original purpose?
- Will the intended use be communicated to the individuals concerned? If not, why not?
- Is the use of the personal information authorised, enabled, or required by legislation?
- What training has been provided to staff on the use of information?
- Can you achieve what you need to do with anonymised information?

Common risk examples (Use)

- Information provided for one purpose may be used inappropriately
- Individuals may be surprised or upset by an unanticipated secondary use and any implied "consent" to a secondary use may not be valid
- Ill-defined purposes result in ad-hoc use in a manner unrelated to the original intended use
- Personal information collected on behalf of another agency is used without legal authority.

Possible mitigations to enhance privacy (Use)

- Clearly define the proposed information use and convey that to the individuals concerned
- Check that any proposed uses won't breach contractual or implied confidentiality undertakings
- Develop robust access control protocols that limit access to a "need to know" basis so that users can access only the information they need for their legitimate functions
- Ensure that access controls are updated constantly and quickly, to accommodate departing staff, changes in roles, and the expiry of contractors' terms
- Provide for regular auditing of access by both authorised and unauthorised users
- For voluntary secondary uses, consider seeking consent first. Ensure that the voluntary nature of any choices is clearly communicated by providing opt-in rather than opt-out mechanisms
- When relying on consent to a secondary use, ensure there is a workable mechanism by which a person who refuses consent, or provides conditional consent, can be recognised

- Ensure that secondary uses are provided for by statutory authority or contractual terms
- Ensure that you have included all routine uses in an appropriate privacy notice
- Make it easy for people to see what you’re doing with their information – make it easily available to them and invite their comments.

Principle 11 – Disclosure of information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds, the specified exceptions apply.

What Principle 11 means in practice

Keep the control – only share information if that's why you got it

You can disclose information for a particular purpose if that's one of the purposes you originally collected it for. However, if you're being asked to disclose for a different purpose, check that you have a good reason and legal authority to do so.

Nobody can use principle 11 to force you to disclose information. Only other statutes or court orders (such as warrants) can make you give information to anybody other than the individual whose information it is. However, principle 11 allows you to disclose information to other organisations if one of the exceptions applies.

The exceptions include:

- where you need to disclose information to an appropriate authority to protect someone (for instance a child who may be at risk)
- where the individual concerned has authorised you to disclose the information to someone else (or you're disclosing it to them)
- where the original source of the information is already publicly available
- where it is for statistical or research purposes and the individual concerned won't be identified
- where disclosing the information is necessary to enforce the law or for court proceedings, or to protect public revenue.

However, as with the use of information (principle 10), these exceptions should be applied on a case-by-case basis and shouldn't be used to justify bulk or regular information-sharing.

Key questions to ask

- Are you creating or changing any information-sharing arrangements with other organisations?
- Is the purpose of disclosure directly related to the original purpose of collection?
- Will information be disclosed as individual records, or in bulk files or aggregated?
- Will personal information be disclosed routinely? For what purpose?
- Is that purpose required, enabled or authorised by any law?
- Whose information will be disclosed or exchanged, and how might that affect them?
- Will the subject be aware their personal information will be disclosed for this purpose?
- Would other disclosures also be contemplated from time to time?
- How will information be exchanged, and what security measures will ensure it's transferred safely?
- If information matching may be required, what databases would be involved?
- What information will be retained in the system once it's transferred?

Common risk examples

- Incorrect or inaccurate information is shared with other agencies
- Non-compliance with statutory or contractual obligations or implied confidentiality undertakings results in breach of trust
- De-identification of personal information before disclosure doesn't prevent re-identification
- Information with negative connotations is shared with another party leading to embarrassment, stigma, or damage to a person's reputation
- Risk aversion means you don't share information that you should be sharing, for instance to protect someone's safety
- Concerns over personal safety arise if sensitive information about a person's activities or whereabouts could fall into the wrong hands
- Secondary disclosure is not necessary or legally justifiable

- Individuals don’t have an opportunity to question the manner in which data received from another agency has been processed to arrive at an adverse decision
- People are unaware of, or have failed to opt out of a voluntary secondary disclosure
- Information is disclosed for a use not directly related to the primary purpose of collection
- Individuals may be surprised or upset by an unanticipated disclosure for secondary use.

Possible mitigations to enhance privacy

- Ensure that appropriate privacy protections are transferred along with the information you’re disclosing, through contractual arrangements or terms and conditions in sharing agreements or Memorandum of Understandings (MoUs)
- Ensure that secondary uses have appropriate statutory authority or contractual terms
- If you’re transferring data to another agency, ensure that its records-management processes have levels of protection that are similar to or greater than what your own organisation requires
- Remove unnecessary identifying details before releasing the information to ensure that it can’t be matched to other information that could establish an individual’s identity
- Put clauses in contracts prohibiting use of anonymised information in a way that could re-identify someone
- Ensure that each participating organisation has a lawful authority to collect and/or disclose the information, and check that proposed disclosures won’t breach secrecy provisions or other restrictions in governing legislation
- Be open with individuals (in advance, if possible) about information-sharing arrangements, and where possible, make secondary disclosures to third parties voluntary – that is, seek consent first
- For voluntary secondary disclosures, provide opt-in rather than opt-out mechanisms and ensure that the voluntary nature of any optional choices is clearly communicated
- Ensure you’ve included all foreseen routine disclosures in an appropriate privacy notice
- Use stakeholder consultation to test community expectations about proposed disclosures.

Principle 12 – Cross-border disclosure

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

- Is subject to the Privacy Act because they do business in New Zealand.
- Is subject to privacy laws that provide comparable safeguards to the Privacy Act.
- Agrees to adequately protect the information
- Is covered by a binding scheme or is subject to the privacy laws of a country prescribed by the New Zealand Government.

What Principle 12 means in practice:

Personal information sent overseas must have privacy protections

There are rules around sending personal information to organisations or people outside New Zealand.

You may only disclose personal information to another organisation outside New Zealand if you are sure that the receiving organisation:

- is subject to the Privacy Act because they do business in New Zealand
- will adequately protect the information, for instance, by using model contract clauses, or
- is subject to privacy laws that provide comparable safeguards to the Privacy Act

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

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

Principle 12 does not apply if the personal information:

- Is sent to a person or organisation that is subject to the New Zealand Privacy Act
- is sent to an agent for storage or processing, or
- is sent to the person concerned (or authorized representative), or
- is publicly available, or
- another law authorises the disclosure.

Key questions to ask

- Does your organisation plan to share information with an overseas company (for purposes other than storage)?
- Do you sell personal information to a business in another country?
- What are the privacy laws in the country where you are sending the personal information? Are there any significant key differences to New Zealand's privacy law?
- Has the individual who the information is about authorised the disclosure? Did they understand their information would be sent to an organisation that may not have the same privacy safeguards as in New Zealand?
- Is the business receiving the personal information carrying on business in New Zealand (and therefore subject to the New Zealand Privacy Act)?
- Do you have an agreement with the overseas business that you could insert clauses providing for privacy safeguards?

Common risk examples

- Your organisation sells personal information to overseas organisations

Possible mitigations to enhance privacy

- Create an agreement with the overseas organisation to provide for privacy safeguards (you can use the model contract clauses on our website to create your agreement)
- Contract a privacy professional or lawyer to review the privacy law in the country where you plan to send personal information
- Clearly explain to the person when you are collecting their information that the overseas company receiving their personal information might not protect the information in the same way as a New Zealand organisation would. Use language that is easy to understand and ask for their consent to send their information overseas.

- Decide to only share or sell personal information to organisations within New Zealand or countries with strong privacy laws.

Principle 13 – Use of unique identifiers

An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any 1 or more of its functions efficiently. Where a unique identifier is to be assigned it must comply with specific conditions.

What Principle 13 means in practice

Be unique – don't use other agencies' personal identifiers

A unique identifier (usually a number) is a record assigned by an organisation to uniquely identify an individual in their interactions with the organisation. You should only assign unique identifiers where this is expressly permitted and necessary for you to carry out your functions efficiently. You should not use unique identifiers that have been developed by another organisation, or for another purpose, unless there is an explicit authority to do this and it's necessary for the purpose of your project.

Limiting the use of unique identifiers reduces the risk that a universal identifier will be established that could be used to link a wide range of information about an individual without their knowledge or control. It also decreases the risk of identity fraud.

Key questions to ask (Unique identifiers)

- How will individuals be identified? Will a unique number or other identification device be used?
- Could the method of identifying individuals result in more than one person being assigned the same information (for example, through information on identities being inappropriately merged)?
- Are you using the same unique identifier as another organisation, such as a tax number, or student number? If so, where is your authority to do so?
- Will any identifying number create a unique record across the population that could be used to link other unrelated personal information to expand an individual's visible profile?

Common risk examples (Unique identifiers)

- Service provision is conditional on supply of a unique identifier assigned by another agency
- Unrelated information about an individual can be linked by association through the use of another agency's unique identifier
- Use of the same unique identifier by different agencies creates a de-facto universal unique identifier.

Possible mitigations to enhance privacy (unique identifiers)

- Only collect a unique identifier provided by another organisation if you have specific legal authority to collect it and you need a record of the number to perform your functions
- Check that the unique identifier has been designed with your intended purposes in mind – is it fit for the purpose to which you're putting it?
- If you need to verify eligibility by using identifiers issued by another organisation, note that the identification has been sighted but do not assign the number to the individual for your own use
- Ensure that your records-management systems are not designed to use unique identifiers issued by another organisation as the primary means of identifying the individual (for example, as part of a matching algorithm)
- Use agency-specific unique identifiers when working across different business units within an organisation to minimise the use of identifying personal information
- Minimise the amount of human-readable or attributable information by use of unique identifiers and other identification methods such as bar codes
- If using another agency's unique identifier to match data, use it as an attribute, not as your primary identifier for your organisation's processes.