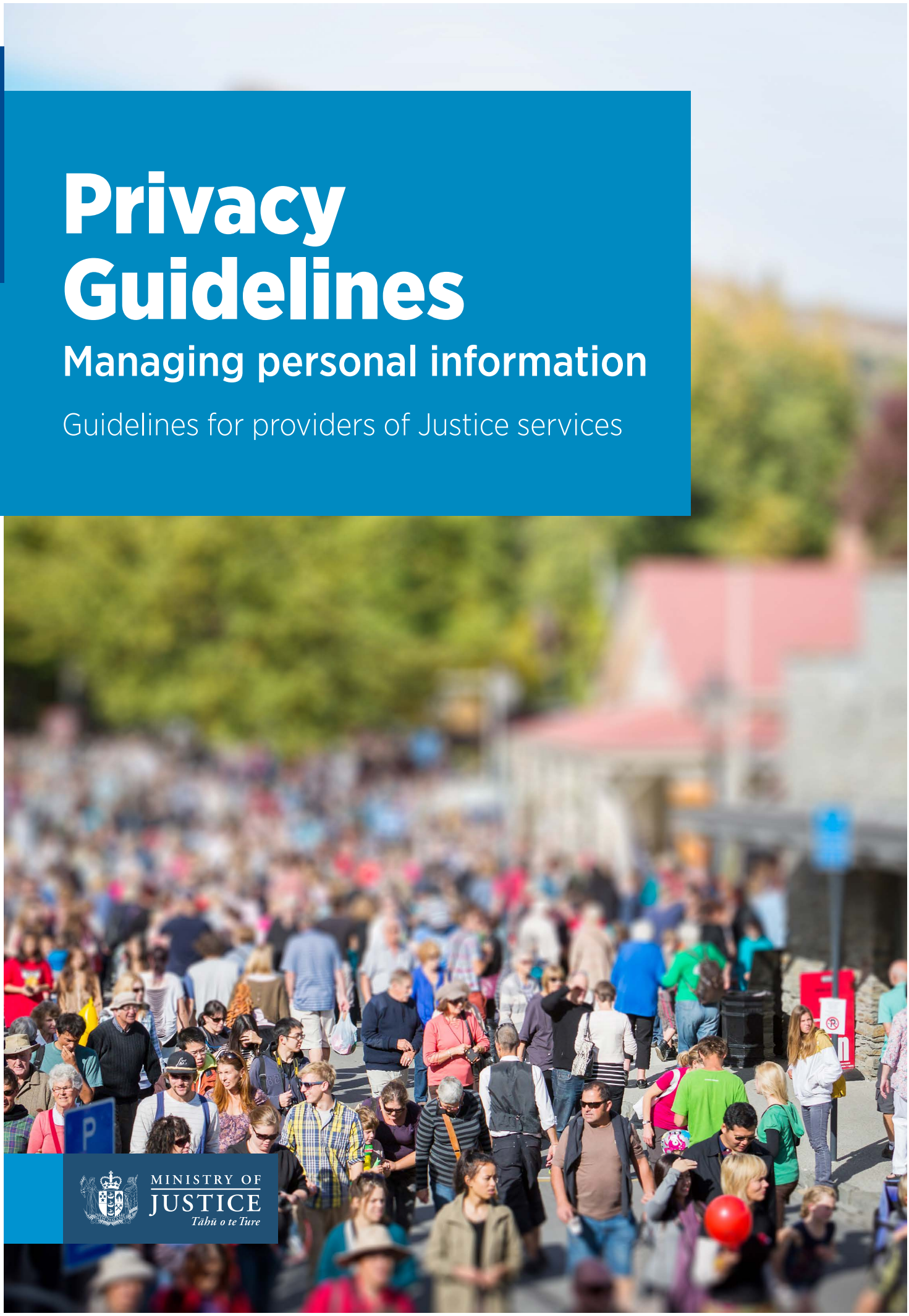
Privacy Guidelines

Managing personal information

Guidelines for providers of Justice services



MINISTRY OF JUSTICE
Tāhū o te Ture

Foreword

We all have a part to play in collecting, sharing or using people's information in a way that respects and protects their privacy.

People who interact with our justice system often do so under difficult and stressful circumstances. It's crucial we respect their confidentiality and treat their personal information with the same respect we'd expect others to treat our own.

If we don't get this right we could, at best, damage people's trust and engagement in the justice process. At worst, we could be putting people's safety at risk.

Our Ministry is responsible for ensuring the personal information our partners collect and share is appropriately managed.

We've developed these guidelines to provide clear guidance for our partners about our Ministry's expectations in terms of privacy and information management. To make things easier, the guidelines include:

- a combination of legislative requirements and best practice standards from across a range of existing privacy, information management and data security resources
- practical suggestions for how you can protect the information of people engaged in justice processes on a daily basis
- real case study examples to help you learn from the experiences of others.

This is the first time we've clearly identified the data security controls we think our partners should have in place to protect people's personal information. Many of you will already have these in place.

We recognise that some of the controls may not be appropriate for the type or size of your organisation. We also acknowledge that some of you will need time and support to put the recommended controls in place.

Our Ministry will work closely with you and your team as we implement these guidelines.

(These guidelines are not a substitute for legal advice.)

Contents

Privacy and information security expectations

This page summarises the Ministry of Justice's expectations for providers of justice services. Our expectations are explained in more depth throughout sections 1-5 of these guidelines.

1

Comply (and be able to show you comply) with the Privacy Act 2020, including, but not limited to:

i. informing people who engage with your services of their privacy rights, including what information they are and are not required to share with you and what you'll do with their information
ii. only collecting, using and sharing information lawfully and for the purposes of delivering your service
iii. maintaining accurate records and verifying the accuracy and relevance of information before using or sharing it
iv. securely disposing of information when you no longer have a lawful reason to keep it
v. allocating one person within your organisation to have overall responsibility for privacy-related issues.

2

Adequately protect the information you collect, use, share and store by:

i. having documented IT policies, processes and controls in place, including maintaining an up-to-date IT security self-assessment
ii. physically securing paper files and IT equipment
iii. protecting your devices and files from unauthorised access or loss
iv. ensuring information is only accessed by those who need it, and regularly reviewing your organisation's access permissions.

3

Have controls in place to ensure only appropriate personnel have access to personal information by ensuring personnel:

i. are suitable for the roles they hold, including completing regular Police and Ministry of Justice criminal record check checks as appropriate
ii. complete the Office of the Privacy Commissioner's 'Privacy ABC' e-module or equivalent at least every two years
iii. know when and how to report a privacy or cyber security incident, or a conflict of interest.

4

Ensure that any actual, potential or perceived conflicts of interest are appropriately managed by:

i. documenting the steps you've taken, and will take, to mitigate any identified conflicts of interest
ii. ceasing any involvement with a case if you're unable to adequately manage a conflict of interest.

5

Respond appropriately to a privacy or cyber security incident, including but not limited to:

i. acting in a timely manner to reduce the loss of information, or unauthorised access to information
ii. reporting privacy and cyber security breaches appropriately.

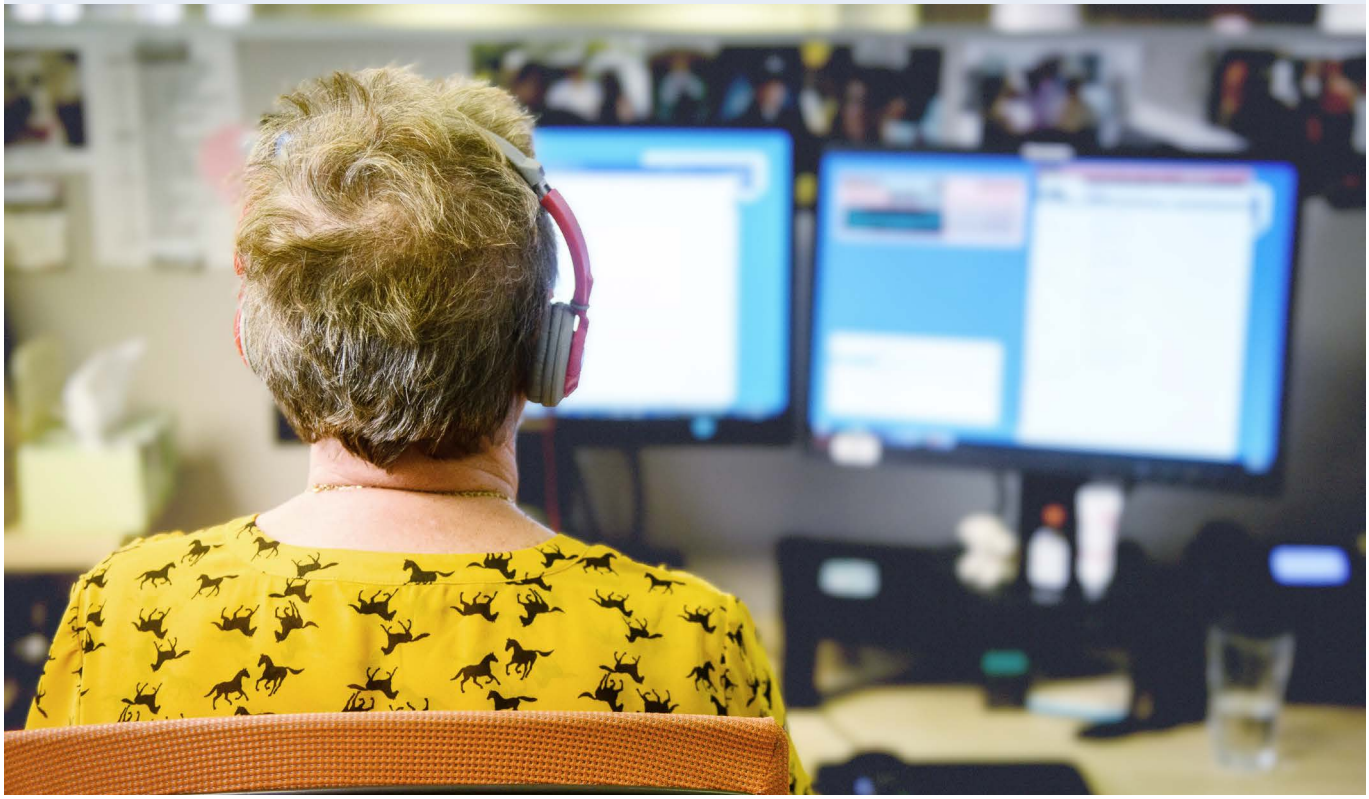
SECTION 1

How to comply with the Privacy Act

This section covers collecting, using, sharing and disposing of information.

The Ministry expects you to comply (and show you comply) with the Privacy Act 2020 (the Act) by:

i. informing people who engage with your services of their privacy rights, including what information they are and are not required to share with you, and what you'll do with their information
ii. only collecting, using and sharing information lawfully and for the purposes of delivering your service
iii. maintaining accurate records and verifying the accuracy and relevance of information before using or sharing it
iv. securely disposing of information when you no longer have a lawful reason to keep it
v. allocating one person within your organisation to have overall responsibility for privacy-related issues.



Privacy basics

Privacy rights

Everyone engaging with our justice system has privacy rights that we must uphold. People can reasonably expect that their personal information is collected, used, and shared respectfully, and adequately protected.

The Privacy Act 2020 affords privacy rights to every New Zealander. These rights include:

- their personal information is only collected, used and shared for legal purposes
- they can access any personal information an organisation holds about them
- they have the right to correct any information held about them.

The Privacy Act:
13 principles to guide good practice

The Act sets out 13 privacy principles that every organisation dealing with personal information must follow. Failure to meet any of these principles is considered a privacy breach.

1. Only collect the personal information you need to carry out a function of your organisation.
2. Where possible, get it directly from the person it's about.
3. Tell the person what you're going to do with it.
4. Collect it legally and fairly.
5. Take care of it once you've got it, and keep it secure.
6. Allow people to see their own information if they want to.
7. Correct it if it's wrong.
8. Make sure it's accurate, up to date and relevant before you use it.
9. Securely dispose of it when you no longer have a lawful reason to keep it.
10. Use it for the purpose you collected it.
11. Only share it for a lawful reason.
12. Only transfer it to an offshore entity that is subject to privacy laws with comparable safeguards to New Zealand's.
13. Only assign and use unique identifiers as permitted.

For the full text of the principles go to:
Privacy Act and Principles

What is ‘personal information’?

Personal information is any information that tells us something about a living, identifiable person.

It doesn’t matter what form the information is in. It may be hardcopy, digital, verbal or even an image. If a person can be identified from it, it’s their personal information.

The information doesn’t have to be sensitive to be personal, and it doesn’t need to include their name if they can be identified in other ways.

Personal information can include:

- address and other contact details
- a person’s image
- references to them in emails or other correspondence
- financial information, such as bank account details, wages, debt, or fines information
- audio recordings of them, such as phone calls
- complaints or comments made about them by other people
- notes taken from conversations, interviews, or other interactions with them
- information ‘held in the mind’ about them, such as recollections of a conversation or interaction with or about them.

You must appoint a Privacy Officer

The Privacy Act requires that every organisation must appoint a Privacy Officer.

Everyone in your organisation should know who this person is and what their responsibilities are. If you’re a sole provider and have no other staff or volunteers, you’ll need to hold the responsibility of Privacy Officer yourself. It’s not as daunting a task as it may sound!

Read more about resources for Privacy Officers

Case Study

A GP’s office sent a follow-up letter to a patient after referring them for counselling for historic abuse. However, they sent it to the wrong street number and failed to put either the patient’s name or a return address on it. Not knowing who it was for, **the neighbour who received it opened it and inadvertently found out about the patient’s history of abuse**. After the patient complained to the Office of the Privacy Commissioner, the medical centre compensated them for emotional harm and made a range of changes to its practices. These included adding a return address to their envelopes, removing specific references to abuse and other personal issues in letters, and using window envelopes to reduce the chance of transcription errors such as forgetting to write the addressee’s name.

Collecting personal information

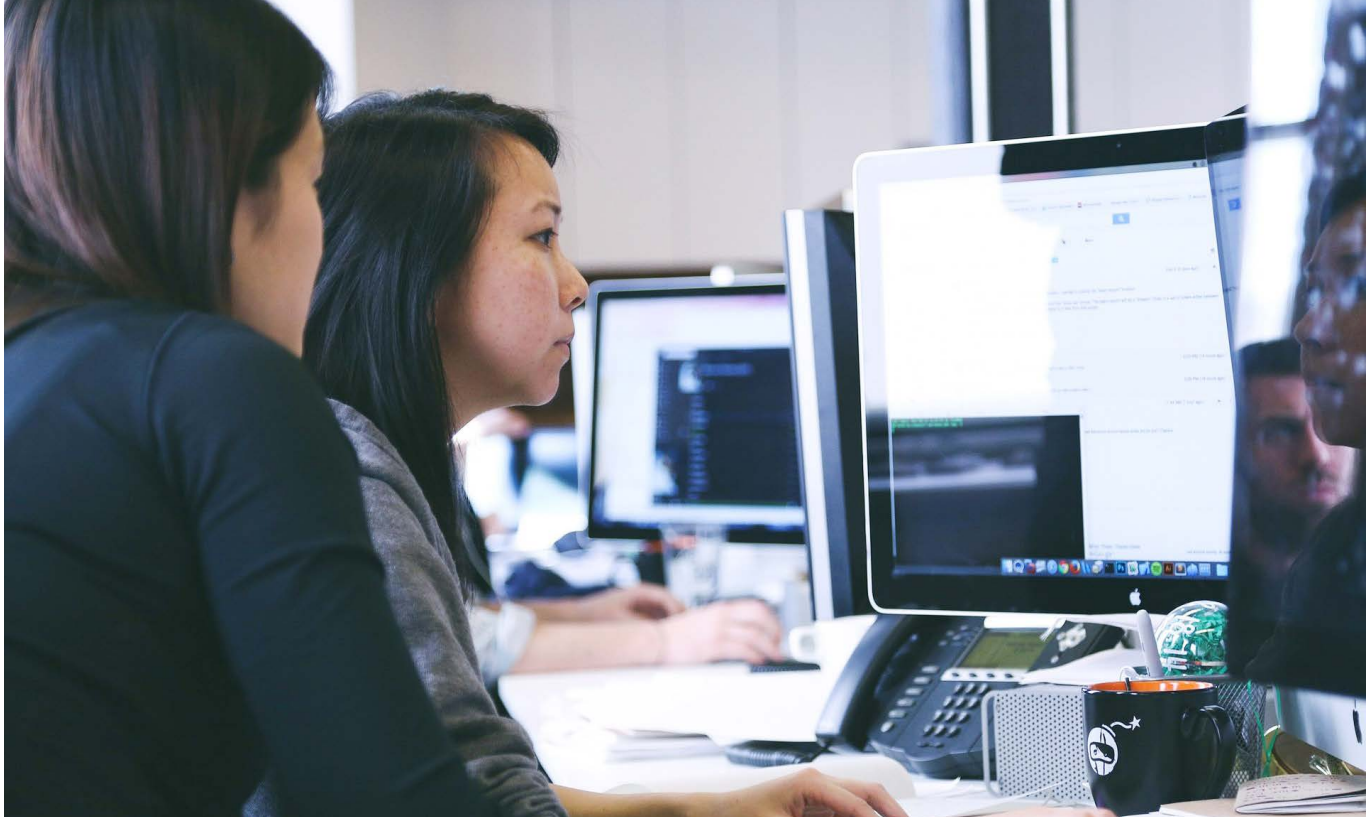
Principles 1-4 of the Privacy Act cover the collection of personal information. In brief, they say you must:

- only collect the personal information you need to carry out a function of your organisation
- where possible, get it directly from the person it's about
- tell them what you're going to do with it
- collect it legally and fairly.

Only collect the information you need

You should only collect the personal information you need to deliver your service. This may include, for example, information from or about clients so that you can provide them with a service; or from or about job applicants to help you decide whether to hire them. This will be information people must provide so that you're able to help them or make decisions in relation to them.

Let people know whether they have to provide the information or whether it is optional. Information may be optional for people to provide because you don't need it for a purpose directly related to them. For example, this could include information that may help you to improve your service delivery, such as feedback or demographic details to help you better target your services.



Collect it from the person themselves

In general, you should only collect personal information from the person it's about. In many cases, you'll receive information from sources other than the person, for example, the courts, Police or other organisations working with the person.

If you receive information from a source other than the person themselves, you need to document where it came from and be confident that the information is accurate. If the information comes from people that are connected to your client, it's best practice to confirm the information with your client if possible. This helps ensure information is accurate and considers any other relevant factors.

Provide a privacy statement that tells people what you'll do with their information

Be open with people about why you're collecting their information and how you'll manage it.

To ensure that people using your services are informed of their rights, you must provide them with a written privacy statement. This includes making it clear what information they are and are not required to provide, and what you'll do with it.

It's best practice to include your privacy statement on your website (if you have one) or in the public areas of your organisation, so people are able to regularly refer to it.

The Office of the Privacy Commissioner has a tool on its website that can help you create your own privacy statement.

Have a legal purpose for collecting information

If you're delivering a service for our Ministry, then you already have a legal purpose for collecting the necessary information from people to deliver that service.

You must ensure that the information you collect isn't used for any unlawful purpose.

Privacy Statement Generator

Priv-o-matic*

Your privacy statement should tell people:

- that you're collecting their information (if it isn't obvious)
- why you're collecting it
- what law you're collecting it under, if applicable
- who will have access to it, and any other organisation or person/s you may share it with
- whether they can choose not to give it to you
- what will happen if they don't give it to you (for example, you won't be able to provide the service)
- that they can ask to access and correct it, and how to contact you to do this.

* Tool from the Office of the Privacy Commissioner

Using personal information

Access to personal information must be limited to those people who need it to do their jobs.

Where staff or volunteers need access to large collections of information, such as databases, you need to have policies and processes in place regarding access to it. You must take steps to ensure your personnel understand, and adhere to your expectations.

Tips

- ✓ Regularly remind staff that access is for official work purposes only.
- ✓ Regularly check access patterns and follow up on any unusual activity.
- ✓ Conduct random audits to ensure staff are only accessing files for clients they've worked with within a given timeframe.
- ✓ Limit or monitor access to high-profile information, information about staff, or information about people you know a staff member has, or may have, connections with.

Only use the information for the purpose you collected it

Under principles 10 and 11 of the Privacy Act, you may only use or disclose personal information for the purpose you obtained it, or where an exception under this principle applies. Exceptions include where:

- the use or disclosure is directly related to the purpose of collection
- the person concerned authorises it
- the use or disclosure is necessary to avoid prejudice to the maintenance of the law or to prevent or lessen a serious threat to someone.

Ensure it's accurate

Under principle 8 of the Act, you have a responsibility to take reasonable steps to ensure personal information is complete, relevant, accurate, up to date and not misleading before you use or disclose it.

People have the right to access and correct their information

Access

People can ask for their information verbally or in writing. Requesting it in writing usually reduces misunderstandings. Although you may suggest the person does this, it's not a legal requirement. If they ask for it verbally, write it down and check with the person that you've recorded their request correctly.

NOTE: When you receive a request, you need to consider:

- whether you hold the information
- whether you should withhold any, or all, of the information
- when you have to respond by (under the Privacy Act, you must respond as soon as reasonably practicable and within 20 working days), and whether you can provide the information within this time or need to advise of an extension.

Before you release any personal information, the Privacy Act requires you must satisfy yourself of the identity of the person requesting it.

The circumstances in which information should be withheld are covered by sections 49–53 of the Privacy Act.

The circumstances in which you can charge for information are covered in section 66.

Correction

Under principle 7 of the Act, people can ask you to correct information you hold about them.

- If you agree the information is incorrect, you should correct it and pass on the correction to any other person or organisation you've shared the information with.
- If you don't agree the information is incorrect, the person concerned can ask you to attach a statement of correction to it. You should attach this in such a way that the correction they sought is always read with the information. You should also pass the statement on to any other person or organisation you've shared the information with.

Case Study

The Office of the Privacy Commissioner concluded Police had not breached a woman's privacy after a constable contacted an Emergency Mental Health Team (EMHT) after she had presented at a station to complain about how a hospital had treated her. The woman told the constable she had suicidal thoughts and had been discharged while still suicidal. He noted her agitated state and evidence of self-harm on her arms. The constable left the room to contact the EMHT without telling her he was going to do so. She complained to the Office of the Privacy Commissioner, which found the disclosure was justified under principle 11(f)(ii) which says **an organisation can disclose personal information if it considers it necessary to do so to prevent or lessen a serious threat to the life or health of the individual concerned.** The organisation must consider the likelihood of the threat being realised, the severity of the consequences if it is realised, and the time within which it may be realised. The disclosure must be to a person or organisation who can help prevent it. An EMHT was the appropriate organisation to contact in the circumstances, and the Office of the Privacy Commissioner considered Police had made the disclosure in good faith to reduce a serious threat to the woman's safety.

Sharing and disclosing personal information

If a person has provided you with personal information, you need to ensure that it's only shared legally and for the purposes it was collected.

Some basics of sending and sharing information appropriately

- Think about how you send and share information.
- If you're **emailing** personal information to a client or organisation, ensure you have the correct email address. Consider whether the information should be encrypted, or whether it's too sensitive to be shared via email at all.
- If you are **posting** personal information to a client's home or work place you should consider what is on the envelope and whether they may be offended or upset if another person were to see or open the envelope.
- If you're **talking** to someone either in person or on the phone, make sure no one can inappropriately overhear your conversation.

Sharing information with the court and Ministry of Justice

When we engage you to work with, or on behalf of, our Ministry or the courts, we'll let you know what information we expect from you (for example, completed forms or reports).

When you're collecting personal information, you must let the person know what information will be shared with our Ministry or the courts. They can then make informed decisions about what they want to tell you. You also need to let them know the consequences if they don't disclose information you need to deliver your service to them.

Research and evaluation

From time to time, our Ministry and other agencies may want to conduct research to evaluate the services you deliver, including the outcomes for people engaging with your service.

When explaining their privacy rights and how you'll use their information, it's helpful to ask people whether they would be willing to participate in future research.

If people choose not to participate in research, it can be recorded so they're not approached by researchers in the future.

Sharing information with Police

You should contact the Police if you have immediate concerns about someone's health and safety or you need to report a crime. The Police or another law enforcement organisation may also request information from you.

The Office of the Privacy Commissioner has guidance to help you decide when it's appropriate to share information, both voluntarily and in response to a formal request.

Office of the Privacy Commissioner guidance on sharing information

Sharing information in accordance with the Family Violence Act 2018

The Family Violence Act aims to ensure information is shared safely and appropriately within the sector.

If your organisation is listed in the Family Violence Act, you must consider sharing information if you receive a request from another organisation or practitioner within the sector, or if you believe that it may prevent someone from experiencing family violence.

Family violence information-sharing guide

Sharing information in accordance with the Oranga Tamariki Act 1989

The information-sharing provisions of the Oranga Tamariki Act (the Act) came into effect on 1 July 2019. These promote proactive and early sharing of information by agencies and individuals where there is concern about the wellbeing or safety of tamariki.

The information-sharing provisions cover a wide range of professionals. If you work with tamariki or their whānau, you need to be aware of your responsibilities under the Act.

Oranga Tamariki information-sharing guide

Case Study

A woman complained to the Office of the Privacy Commissioner after a social service organisation posted a letter containing personal information about her and her family to her work address. The employer had a policy of opening mail addressed to its employees and the organisation knew this because it had made the same mistake on a previous occasion. The employer disclosed the contents of the letter to the woman's workmates and they used it to bully her. This caused her stress and ongoing medical issues, which affected her ability to do her job. The Office of the Privacy Commissioner accepted that the actions of the organisation in sending the letter to the incorrect address contributed to the harm the woman suffered, and the organisation eventually paid her compensation of $6,000.

If you have further questions about when to share or withhold information, the Office of the Privacy Commissioner operates a freephone line (0800 803 909) or you can always seek your own legal advice.

To help you in deciding what laws apply when you're considering sharing the information of families/whānau and vulnerable children, the Office of the Privacy Commissioner has an escalation ladder to help you work through issues step by step.

Office of the Privacy Commissioner's escalation tool

Keeping accurate records

You have a responsibility to take reasonable steps to ensure personal information is complete, relevant, accurate, up to date and not misleading before you use or share it.

The information you collect may be used to make important decisions relating to your clients and their whānau. It's essential you remain impartial in the way you record it.

The records you keep should be detailed enough to provide the full context and all relevant information so that another person is able to obtain an accurate understanding of the situation.

Confirm information is accurate before you use it

Information can quickly become outdated. Wherever possible, confirm details before you share them with others.

- ✔ Information should be accurate at the time you share it. If you're unsure, make it clear at what point you last confirmed the information.

Record your level of confidence in the information

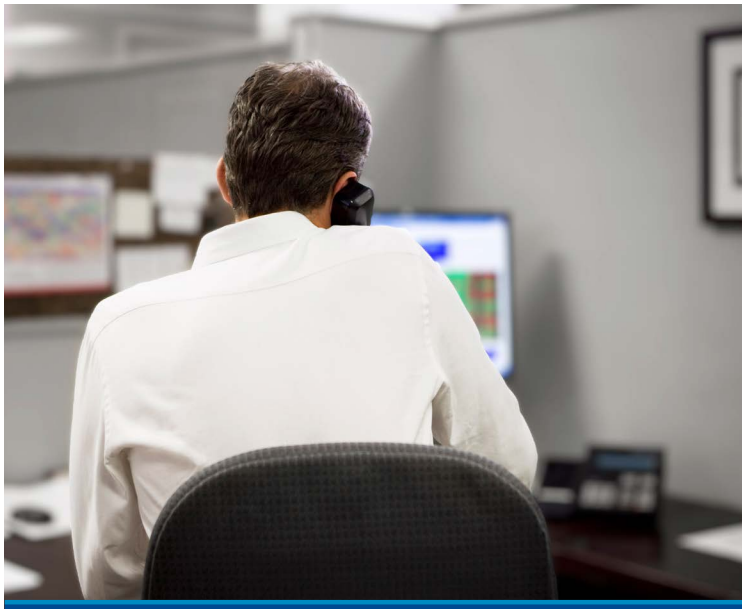
It's important that you write or record information you receive in a way that allows another person to interpret your level of confidence in the information. For example, if you're told by a third party that someone's information has changed, your records should state that it's yet to be confirmed by the person concerned.

- ✔ Recording information in notes as 'stated by X' or 'X suggested…' can help prevent information you hold being incorrectly shared as fact.

Centralise your record keeping

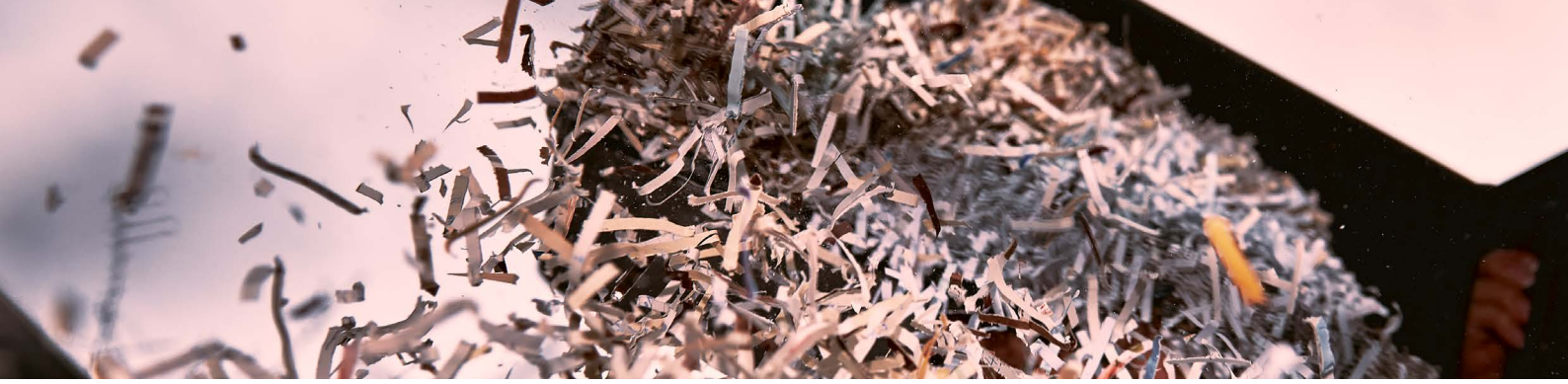
It's important your organisation has clear processes for how it records and stores personal information. There should be only one source of authoritative, reliable information.

- ✔ Clearly and consistently name documents, files, email subjects and notes to help others find and use the information later.
- ✔ Avoid storing important information in multiple places.
- ✔ If you're copying information, make sure the copies are destroyed when no longer needed.



Case Study

A man complained to the Office of the Privacy Commissioner that **a government organisation had incorrect information** that stated he had been jailed for sexual offending. The man contacted the organisation twice to ask for the information to be corrected, yet they continued to use it in reports to the court. The Office of the Privacy Commissioner found **the organisation breached the man's privacy under principle 7 in failing to respond to his requests for correction, and principle 8 for failing to take reasonable steps to check the accuracy of the information it held about him.** It accepted that, due to the nature of the information, he had suffered significant hurt and humiliation as a result of their failings. It referred the man's complaint for consideration by the Human Rights Review Tribunal.



Disposing of personal information

You should only hold information when you have a lawful purpose for doing so.

It can be difficult to know when to destroy or delete old files and information. There are specific requirements for the retention of some records such as health, employment and tax records but these may not apply to services you provide. It can also be difficult separating information so that some can be disposed of and some kept for later.

If you have no immediate need for the information, we recommend you safely store or archive any information you may need in the future.

- Keeping 'active' and 'closed' client information separate can prevent it being accidentally lost, shared or misused.
- Keep any information required for audit processes.
- Keep information relating to an ongoing legal matter, it should be retained in case it's required by the court.

If you have no lawful reason to keep information, you should safely dispose of it. This permanently removes the risk of information being misused or lost. It may be challenging to remove information you no longer need from some case or file management systems. Contact your IT or system provider for advice about what you can do. It may be helpful to consider the data protection and use principles in Appendix One when deciding what you should do.

Safely disposing of hard copy information

Some common ways to dispose of paper files include shredding and using the services of a document destruction company. You must ensure that information is disposed of in a way that doesn't allow anyone to reconstruct the information or see anything that might be considered personal.

Disposing of computers and other devices

Digital information can be more difficult to dispose of as it's not always clear where copies of information exist.

If you delete information, don't assume that the information won't be able to be accessed by someone at a later date.

If you're disposing of computers or other devices, you should:

- destroy them to the point that hard drives are not able to be reconstructed OR
- engage a trusted IT professional to wipe the devices of any data.

Email accounts and web services

Email accounts store all information sent to or from an email address and it's not always easy or practical to delete information from them.

It's important that you retain the ownership of any email account your organisation uses to send or receive personal information.

- When people with access to an account leave your organisation or no longer deliver services associated with an email account, you should remove their access to the accounts.

If your email service provider allows you to safely delete an account, you should have a policy that sets out when it's appropriate to delete accounts and restrict administrator rights.

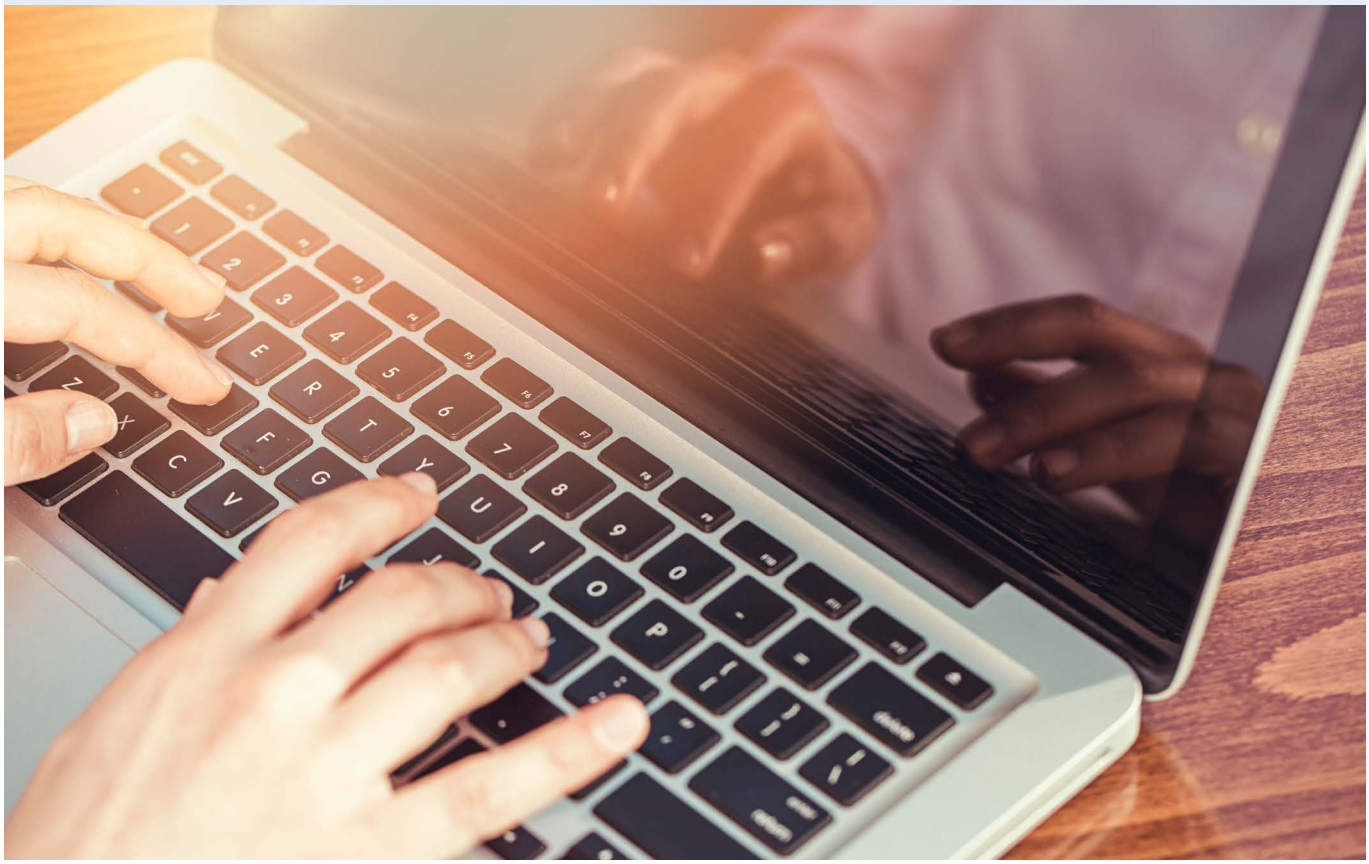
SECTION 2

How to protect information

This section covers our Ministry's expectations for protecting any personal information you collect, use, share and store by:

i. having documented IT policies, processes and controls in place, including maintaining an up-to-date ICT security self-assessment
ii. physically securing paper files and IT equipment
iii. protecting your devices and files from unauthorised access or loss
iv. ensuring information is only accessed by those who need it, and regularly reviewing your organisation's access permissions.

The Ministry of Justice is expected to align with processes and controls essential for the protection of all New Zealand Government information and systems. When sharing information, we expect you to apply the same level of due diligence to ensure personal information is kept secure.



Complete a data security self-assessment for your organisation

There is no 'one size fits all' approach to securing information you hold digitally. We expect you to have adequate controls in place, but 'adequate' will vary depending on the size and structure of your organisation and how you operate.

You should assess your organisation against 28 data security controls we have identified as realistic measures you can take to help keep information safe. Implementing all controls is desirable, however our Ministry considers 16 of the controls to be of highest priority. More information about the assessment can be found in Appendix Two.

Data security steps you can take to keep information safe

There are some straightforward things you can do to reduce the risk of information being disclosed, modified, or made available in an unauthorised manner.

1 Keep information physically safe, especially in transit

Whenever you take information off site, you're exposing it to risk. Information taken out of the office can be accidentally left in a public place, stolen from a vehicle, or lost or misplaced at a destination such as the home of another client.

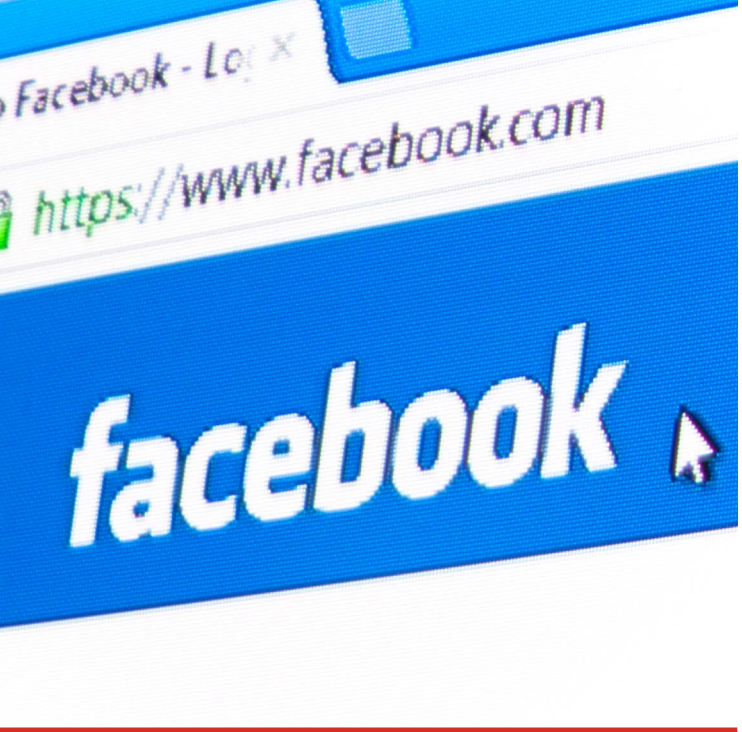
2 Protect your devices from being infected with malicious software

Your devices should have controls in place to prevent malicious software (malware) from being executed. Malware can come from browsing the internet, opening attachments from the wrong email, or using an unauthorised USB. Once installed on your device, malware can access your personal and customer information, deny you access to files, or use your device to spread further infection across the network.

- ✓ Devices you should include when implementing protective controls are laptops, desktop PCs, tablets, mobile phones, servers and network devices.

Checklist before leaving the office

- ✓ Do I have only the information I need?
- ✓ If I've printed anything, have I collected all the information from the printer?
- ✓ If I'm taking information about more than one client or case, do I have them securely separated?
- ✓ Do I need to take a hard-copy file, or do I have a secure way to access the electronic file from my laptop or other device?
- ✓ Do I have a strong password on my device, and is all security and anti-virus software up to date?
- ✓ Is any personal information held on my device password-protected or encrypted?
- ✓ If carrying hard copies, are they secure and do I have my contact details on the outside of the folder, envelope or case so they can be returned without being accessed if I lose them?
- ✓ How am I travelling? What precautions can I take to ensure I don't accidentally leave the information on public transport, in a taxi, or at a stop on the way?
- ✓ How will I keep the information secure when I reach my destination?



Beware

Even the biggest web services are subject to data breaches – in recent years there have been breaches by LinkedIn, Dropbox, Adobe, MyFitnessPal, Forbes and Sony, to name a few. Once services like these are breached, hackers will download the username (which is usually your email) and password list and start using the same email/password combination across other common web services.

We recommend you take these basic steps to stop these types of attacks

- ✓ Don't use work email addresses for logging onto web services
- ✓ Use unique passwords across any services you use
- ✓ Have multifactor authentication applied to your accounts.

See **CERTs page on getting password smart** for more information

3 Encrypt your files and devices

Encryption is used to ensure a device or file can only be accessed by someone that has the key, or password, to decrypt the information. This means that if a device or file does fall into the wrong hands, the unauthorised party won't be able to do anything with the information.

For example, USB drives are portable and convenient to carry around, but they're also easy to lose. If a USB drive is lost and wasn't encrypted, anyone who finds it will be able to access all the files on it. Encrypting USBs with a strong password will greatly reduce this risk.

Case Study

A contractor's home office was broken into and her laptop stolen. The laptop contained files dating back 10 years and included the confidential information of over 80 of her former clients. The laptop had no password or encryption protection to prevent unauthorised access to the information on it.

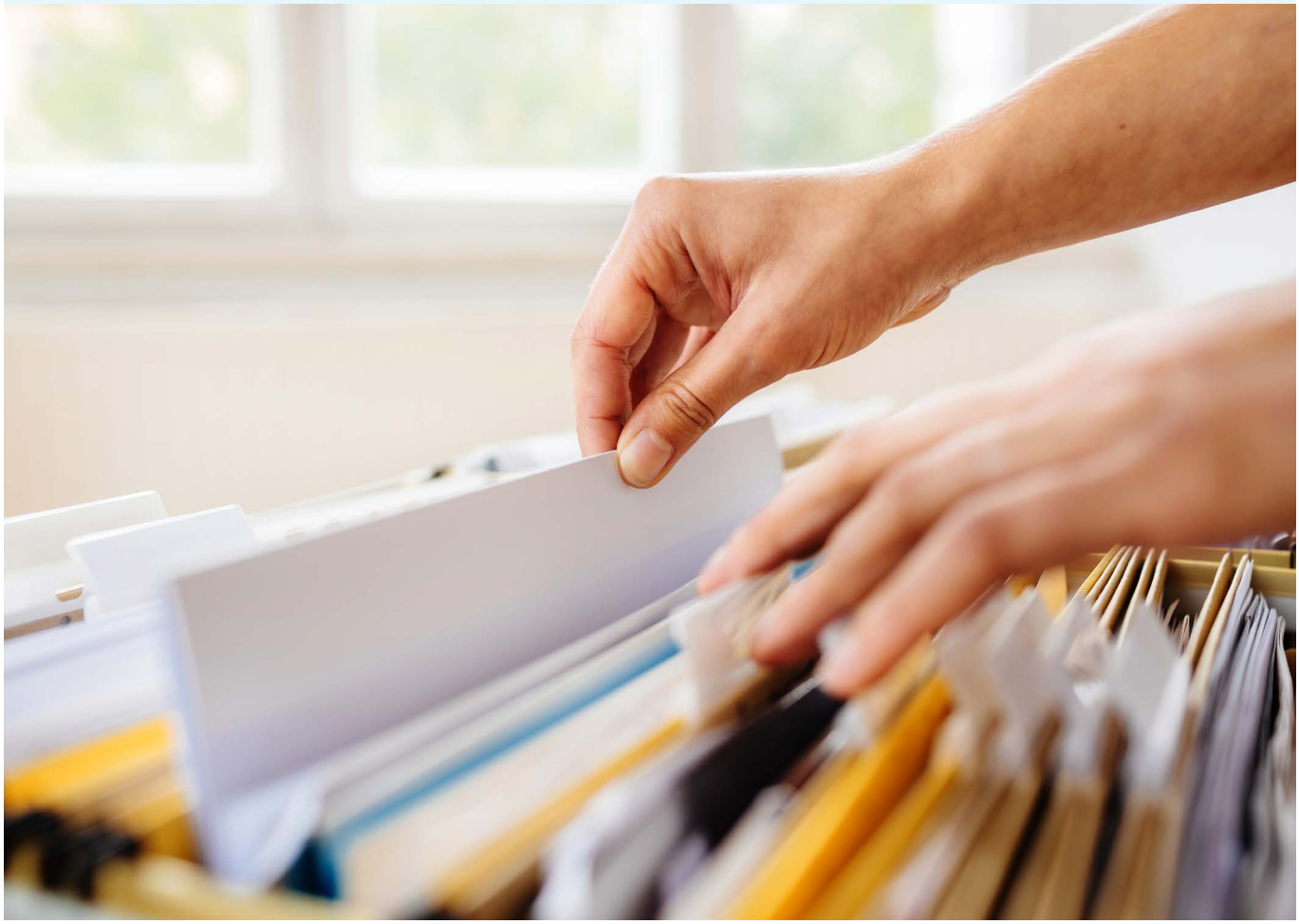
The Office of the Privacy Commissioner was notified of the theft due to the large number of people affected and the sensitivity of the information. The contractor was fined for failing to take adequate steps to protect her clients' information.

SECTION 3

How to manage access to information

This section covers our Ministry's expectations that you have controls in place to ensure only appropriate personnel have access to personal information by ensuring personnel:

i. are suitable for the roles they hold, including completing regular Police and Ministry of Justice criminal record checks as appropriate
ii. complete the Office of the Privacy Commissioner's 'Privacy ABC' e-module or equivalent at least every two years
iii. know when and how to report a privacy or cyber security incident, or a conflict of interest



It's important to develop a culture of respect for people's personal information

Engage suitable people for your organisation

Police and criminal record checks

You should have robust recruitment processes in place to ensure that you have the appropriate staff and volunteers for the work they do and the information they have access to. This includes completing regular Police and Ministry of Justice criminal record checks as appropriate.

People engaging with your services should be able to have confidence in the people within your organisation. You should consider whether it's suitable for people with convictions or pending charges to deliver services. In some cases, your Ministry contract may restrict this.

Give access to information on a 'need to know' basis and regularly review it

Only provide the level of access people need to do their job – this is known as the principle of least privilege. This reduces the risk of unauthorised access to personal information.

Accounts for personnel should be set up to require strong passwords.

Controls such as multifactor authentication can ensure that even if a password is obtained by an attacker, an additional step (such as further information) is still required to access that person's account.

Case Study

A health organisation **paid compensation to an ex-employee and strengthened its monitoring processes after a routine audit showed two colleagues had accessed her health records without proper reason**. The records her colleagues had 'browsed' included extremely sensitive medical information, which had been accessed over a period of time. Although the organisation responded in a proactive, sympathetic and responsible way to the interference with the woman's privacy, it accepted it had limited processes in place to monitor inappropriate access to its files. It initiated an independent review of its health records audit process and implemented the resulting recommendations.

Privacy and IT security training for your personnel

We expect all people involved in the delivery of justice services, who have access to people's information, to have completed basic privacy training. The Office of the Privacy Commissioner has a range of online e-modules that are available free of charge. At the completion of each module, participants receive a certificate of completion that can be kept on file.

The Office of the Privacy Commissioner's 'Privacy ABC' or an equivalent level of training should be completed at least every two years. **Free e-learning**

Privacy training checklist

Key things all personnel in your organisation should know.

- Who your Privacy Officer is. This could be advertised on a poster or staff intranet.
- Your policies and systems around privacy.
- The basic principles of the Privacy Act and how they apply to the work they do.
- How to identify a privacy breach, cyber security incident or conflict of interest and what they should do next.

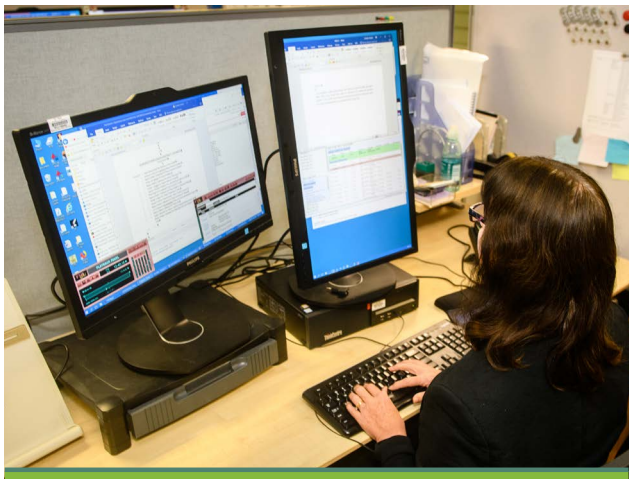
Ensure your personnel are trained to use your IT systems and understand basic IT security

CERT NZ has a wide range of useful material and advice on their website.

- Cyber security awareness for your staff
- Get password smart

Additional information can be found on Netsafe's website, such as:

- scams
- staying safe on social media



Basic IT security training checklist

Key things all personnel in your organisation should know.

- Your IT policies and systems around data security.
- The importance of having strong passwords.
- The risks of sharing personal information on social media.
- How to identify common cyber-attacks such as phishing, targeted and scam emails, and to be alert to other cyber threats like rogue USBs.
- The limitations of email for sharing personal information.

Building a culture of privacy and data security in your organisation

To develop and maintain a strong culture within your organisation, it's important that privacy and data security are kept at the front of people's minds. Some of the resources already mentioned on the Office of the Privacy Commissioner, CERT NZ and Netsafe websites can help you do this.

Each year, there is a 'Privacy Week' and a 'Cyber-security Week' and these provide opportunities to educate your staff and volunteers and reinforce good practices. Our Ministry will send out reminders and resources during these weeks to support you.

SECTION 4

How to manage conflicts of interest

This section covers our Ministry's expectations that any actual, potential or perceived conflicts of interest are appropriately managed by:

i. documenting the steps you've taken, and will take, to mitigate any identified conflicts of interest
ii. ceasing any involvement with a case if you're unable to adequately manage a conflict of interest.

Conflicts of interests occur as a normal part of life, but they need to be managed so they don't lead to conduct that's unfair, biased or even criminal.

The Ministry of Justice is responsible for ensuring New Zealanders have fair and equal access to justice. All our Ministry partners must not only behave ethically but be seen to be doing so.

Identifying conflicts of interest

As Aotearoa New Zealand is a small country made up of many small communities, it's not unusual for conflicts of interest to arise. A conflict of interest can happen in a number of ways - for example, through a relationship, an activity, or even personal beliefs.

As our Ministry partner, you could be compromised in carrying out work on our behalf, if you're required to deal with:

- a relative or close personal friend
- an organisation, club, society or association you belong to
- a person who is your church or community leader
- a person or organisation:
  - you have a professional or legal obligation to
  - you have a business interest or own property with
  - you owe money to
  - you currently or have previously worked for.

A conflict of interest can be:

actual: where the conflict already exists

potential: where the conflict is about to happen, or could happen

perceived: where other people might reasonably think that a person has been compromised.

Responding to conflicts of interest

You must address any actual, possible or perceived conflicts of interest in a transparent way. People engaging with our justice system shouldn't feel like they're being treated unfairly because of another person's personal interests.

Options for managing conflicts include:

- **restricting involvement**: imposing restrictions on the person's further involvement in the matter
- **reallocating responsibility**: replacing yourself or the person concerned with an independent third party for part or all of the process/service
- **removing the conflict**: if appropriate, a conflicting private interest may be relinquished so that a service can be delivered
- **relinquishing the work**: when you and/or your organisation can't resolve a conflict, we'll need to find another party to deliver the service.

There is a useful template to help you manage a conflict of interest in **Appendix Three**. You can use your own form if you prefer.

Reporting conflicts of interest

Not all conflicts of interest should, or need to, be reported to us. We expect you to manage most instances without our Ministry needing to become involved.

We expect that if anyone were to complain about a conflict of interest relating to services you're providing as our Ministry partner, you could produce a clear record of how you managed the issue and the steps you undertook to mitigate any concerns.

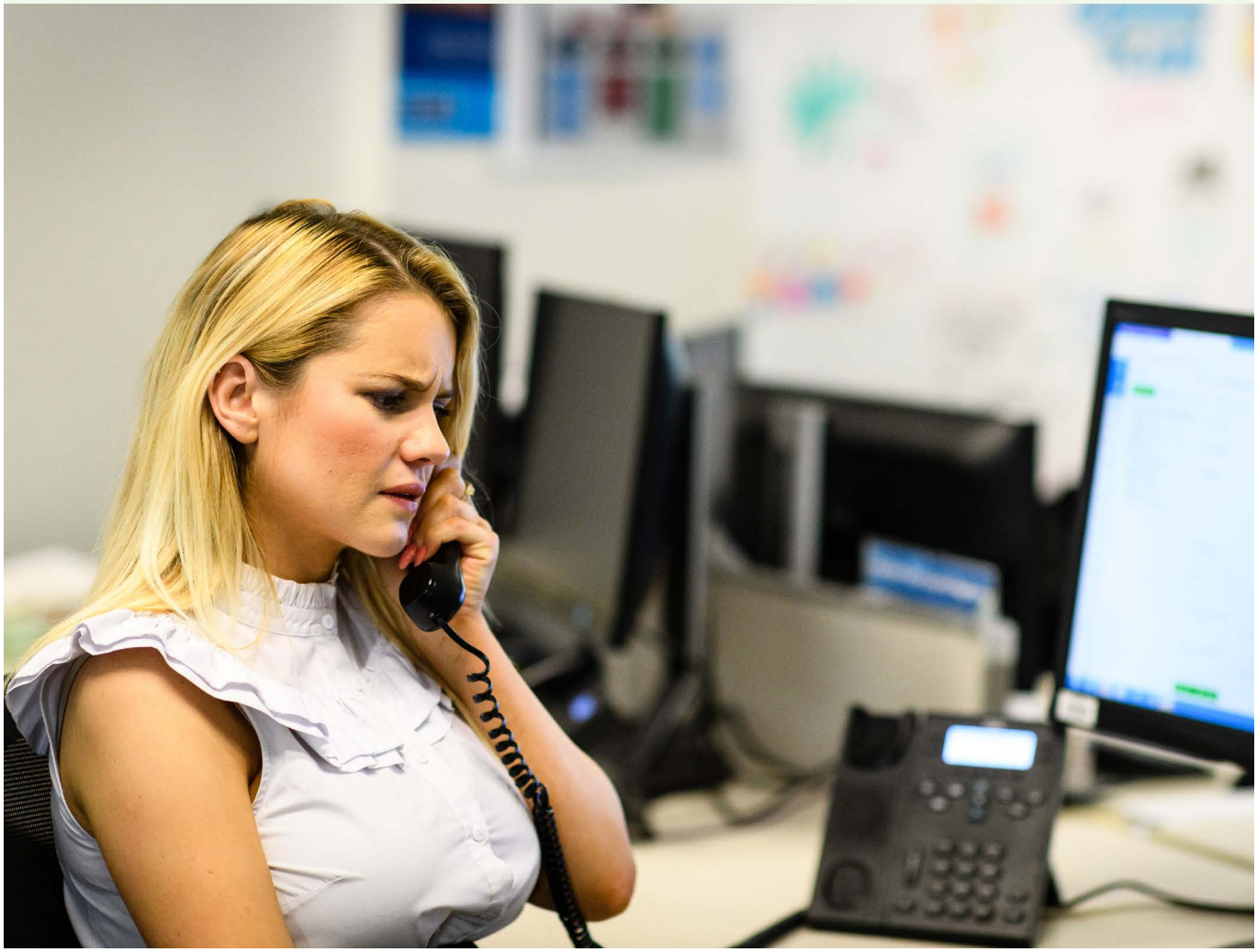
If you're unable to adequately manage a conflicting interest, we expect you to inform us. We'll work with you to either manage the conflict or find someone else to deliver the service. This can be done by contacting your Ministry contract manager, talking to the court that allocated the case to you, or contacting 0800 COURTS (0800 268 787) for more information.

SECTION 5

How to respond to privacy and cyber-security incidents

This section covers our Ministry's expectations regarding responding appropriately to a privacy or cyber-security incident, including:

i. acting in a timely manner to reduce the loss of information, or unauthorised access to information
ii. reporting privacy and cyber security breaches appropriately.



Identifying privacy breaches

A privacy breach (or incident) is where an organisation breaches any of the privacy principles. This includes, for example, failing to respond to an access or correction request within 20 working days, and retaining personal information for longer than you have a lawful purpose for doing so.

Most commonly, however, privacy breaches involve information being lost, shared, altered, destroyed, or otherwise compromised.

Personal information being accessed or used without authority, such as staff looking up other people's information for personal or other unauthorised reasons, is also a breach of privacy.

A privacy breach may involve:

- personal information about one or more people being mistakenly or accidentally sent to the wrong person or persons
- removable storage device/s, laptop/s, or hard copy files containing personal information being lost or stolen
- employees inappropriately accessing and/or sharing personal information
- databases/datasets containing personal information being hacked or illegally accessed
- files being lost in transit.

Cyber security incidents

If a cyber security incident or breach has occurred on one of your devices, you may need to involve an IT specialist to understand the full extent of the breach and mitigate any harm or future risk.

CERT NZ lets you report an incident. They can help you identify the issue you are having and let you know what the next steps are to resolve it.

If the issue relates to any Ministry system or if it results in a privacy incident, then you need to make sure you notify the Ministry as soon as it is practical to do so.

Responding to a privacy breach or incident

There are five key steps to work through after you become aware of a privacy breach:

1 Contain the breach and make a first assessment

- What information was involved?
- Do you know who has it?
- Can you recover it, or confirm it has been deleted or destroyed?

2 Evaluate the breach

- Have you been able to recover or confirm destruction of the information?
- How many people's information is involved?
- How sensitive is the information?
- Could anyone be harmed by misuse of the information if it's not recovered (for example, threats to physical safety, identity theft, hurt or humiliation)?
- Does it meet the criteria for reporting to the Office of the Privacy Commissioner?

3 Report the breach

- Once you've established that a breach has occurred, you need to begin reporting the incident.

4 Notify affected people if necessary. Consider:

- whether you've been able to contain the breach (recovery/deletion)
- who the information went to, if known
- the potential for harm to them if the information is misused
- whether telling them is likely to cause more harm than not telling them.

5 Analyse what caused the breach and take steps to prevent it happening again

- Don't stop at 'human error' – what changes can you make to your processes or work practices to reduce the chance of the error reoccurring?

Find detailed information about responding to, containing, and preventing privacy breaches in the Office of the Privacy Commissioner's Data Safety Toolkit.

Reporting privacy and cyber security breaches to the Ministry

If you have a breach which affects, or which may affect Ministry clients, you must notify the Ministry.

The Ministry of Justice retains some responsibility for the information it shares with you and even the information you generate on our behalf.

You must inform us as soon as practicable if an incident occurs that may cause harm to a Ministry of Justice client.

Contact your contract manager or the court you're delivering services to as soon as practicable after you become aware of any breach that may adversely affect Ministry clients.

If you're unable to contact either your contract manager or the court in a timely manner, contact our Ministry on 0800 COURTS (0800 268 787). Only sending an email advising of the incident isn't acceptable. You need to receive a response back from us acknowledging what's occurred and the next step in the response.

What will the Ministry do?

We're committed to protecting the privacy of all our Ministry clients and will ensure that everything is done to limit any harm that occurs as a result of a breach.

Depending on the nature of the incident and your ability to manage the situation, we'll help you to:

- identify the extent of the breach
- decide whether there's any further action you or our Ministry needs to take to contain the incident, notify affected people, or manage any reputational risk
- decide whether the Office of the Privacy Commissioner needs to be notified. It may be appropriate for our Privacy Officer to do this if you haven't done so already, but we'll discuss this with you.

Our Ministry will work with you as appropriate to ensure that any incident is properly investigated, and any potential harm is mitigated.

New law requires you to notify the Office of the Privacy Commissioner in some situations

New provisions in the Privacy Act 2020 require that the Office of the Privacy Commissioner is notified of privacy breaches in some circumstances. Notifiable breaches are covered in Part 6 of the Act.

What is considered a notifiable breach?

A notifiable breach is one that it is reasonable to believe has caused, or may cause, serious harm to an affected individual or individuals.

The Privacy Act doesn't define 'serious' harm, but does define 'harm' elsewhere as:

- loss, detriment, damage, or injury
- an adverse effect on a person's rights, benefits, privileges, obligations, or interests
- significant humiliation, loss of dignity, or injury to a person's feelings.

When deciding whether the Office of the Privacy Commissioner will need to be notified of a breach, the following factors should be considered:

- the sensitivity of the information involved, or any potential it may have to be used to cause harm in the circumstances (for example, through identity theft)
- who has, or may have, the information
- how accessible the information is (for example, is it encrypted or password-protected?)
- the nature of the harm that could be caused to the person or people it's about
- what steps you've taken to reduce harm following the breach (for example, have you been able to quickly recover the information and are confident it will not be used or disclosed?)
- any other relevant matters.

When must a breach be notified?

From 1 December 2020, you must notify the Commissioner **as soon as practicable** after you become aware that a notifiable privacy breach has occurred.

See the **Office of the Privacy Commissioner's Data Breach page**, call them on 0800 803 909, or email **enquiries@privacy.org.nz** for more information about when you need to notify them of a data breach.

APPENDIX ONE

Key sources of information

These guidelines bring a wide range of information together to help providers understand the basics of good privacy and information security practice. They don't replace legal advice. There are more comprehensive sources of information that can be freely accessed if you wish to further your knowledge or have specific issues you need more information on.

Office of the Privacy Commissioner

The Office of the Privacy Commissioner works to develop and promote a culture in which personal information is protected and respected.

The **Office of the Privacy Commissioner's website** has a wide range of resources and training material.

Cert.govt.nz

CERT NZ is your first port of call when you need to report a cyber-security problem. They support businesses, organisations and individuals affected by cyber-security incidents, providing trusted and authoritative information and advice.

CERT NZ has some **business basics** to help keep your organisation secure online.

Data Protection and Use Policy

The Social Wellbeing Agency developed this policy in 2019 after engaging with a wide range of social services on the protection and use of data. The policy is based on the following principles which will help you make good decisions about how you collect, use, share, store and protect personal information.

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 appropriate checks and balances and ensure that information is suitable and reasonably necessary for the desired outcome.

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

Kaitiakitanga: act as stewards in a way that is understood and trusted by New Zealanders.

Mana whakahaere: empower people by giving them choice and enabling their access to, and use of, their data and information.

Mahitahitanga: work as equals to create and share valuable knowledge.

The Social Wellbeing Agency has **guidance to help implement these principles**.

Sharing information safely: Guidance on sharing personal information under the Family Violence Act 2018

Many of our partners will meet the criteria as a family violence organisation under the Family Violence Act 2018. If you do, these guidelines will help you be aware of your responsibilities around sharing information safely.

Sharing information safely guidelines

Information-sharing to support the wellbeing and safety of our tamariki

A wide range of professionals are covered by the information sharing provisions under The Oranga Tamariki Act 1989. If your organisation works with tamariki or their whānau, these guidelines will help you understand your responsibilities under the Act.

Information sharing guidelines

Protective Security Requirements (PSR), and the New Zealand Information Security Manual (NZISM).

The NZISM details processes and controls essential for the protection of all New Zealand Government information and systems.

The manual is available from the Government Communications Security Bureau.

Netsafe

Netsafe is an independent, not for profit, New Zealand organisation focused on online safety.

Netsafe has a **range of helpful, free resources** available.

APPENDIX TWO

Data security self-assessment for providers of Justice services

Instructions for using this assessment

- You should complete this self-assessment if you deliver justice services for our Ministry, for example if you are a family violence, restorative justice or community law service provider etc.
- It is a useful but optional resource for legal aid lawyers and one-off providers of court services (such as court report writers).
- Assess your organisation against 28 data security measures that have been identified as realistic measures you can take to help keep information safe. We acknowledge some may not be appropriate for the type or size of your organisation.
- There are two levels of recommended data security controls, priority 1 (orange) and priority 2 (yellow). If implementing changes in your organisation, it is recommended you put in place priority 1 controls first.
- Once completed, please hold the self-assessment form within your organisation for monitoring and audit purposes. We may discuss your assessment with you.
- You should review and update your self-assessment annually, or more frequently if your systems and processes change.
- Footnotes explain IT terms in more detail. Please get in touch if you need any help to complete this form.

Name of your organisation:

Name and role of person completing the self-assessment:

Date of first self-assessment:

Section 1: Educating your personnel about data security

Question	Please indicate which most applies to your organisation	*When were people last reminded of their responsibilities?* 6mth	12mth	24mth	24mth+	Comments (including any reasons the recommended control is not applicable to your organisation)
1. Are people aware of common cyber-attacks? This includes hacker tactics such as fraudulent emails (phishing), infecting systems with rogue USBs (baiting), fake IT support calls seeking passwords (quid pro quo), tricking people into thinking they have been hacked so they download infected software (scareware) etc.	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	

Question	Please indicate which most applies to your organisation	*When were people last reminded of their responsibilities?* 6mth	12mth	24mth	24mth+	**Comments** (including any reasons the recommended control is not applicable to your organisation)
2. Are people aware of the importance of using strong passwords[1]?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
3. Do people know how to report a cyber security incident?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	

Section 2: Protecting your devices and files from unauthorised access or loss

Question	Please indicate which most applies to your organisation	*If you have a plan for putting this control in place, when?* 6mth	12mth	24mth	24mth+	**Comments** (including any reasons the recommended control is not applicable to your organisation)
4. Is encryption[2] applied to all your portable devices? (i.e. passwords on all laptops, phones, tablets and USB drives)	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
5. Are your operating systems and applications, including patch management[3] up to date for all devices?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
6. Do all your devices have up-to-date antivirus[4] protection?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
7. Are Microsoft Office macro settings configured to allow only trusted macros[5] on all your devices?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	

1 **Strong passwords** are passwords that are difficult for others to guess, typically involve unpredictable phrases, or the use of multiple character types such as capitalisation, numbers and special characters such as #,?, <, % etc). CERT NZ provides guidance at **https://www.cert.govt.nz/business/guides/policies-and-processes/password-policy-for-business/**

2 **Encryption** is the encoding or 'scrambling' of information so that it cannot be accessed by people who don't have the right key (password) to decrypt it. Encryption can be applied to network traffic, files, folders, portable drives, or entire devices. Microsoft provides guidance on encrypting files at **https://support.microsoft.com/en-us/help/4026312/windows-10-how-to-encrypt-a-file**.

3 **Patch management** is the process of ensuring that vulnerabilities that have been identified in software or devices you use are corrected promptly, by regularly installing security updates released by vendors. CERT NZ provides guidance at **https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/keep-up-with-your-updates/**

4 **Antivirus** products can detect and block many forms of viruses and other malware hidden in files. Ensuring that all devices (computers, phones, laptops) have antivirus products installed and constantly kept up to date will help to ensure they are adequately protected from malicious files.

5 **Macros** are small applications that can run inside larger applications – usually within Microsoft Office documents such as Word, Excel and PowerPoint. When used maliciously in a document, macros have the potential to delete files, upload data, or download further malicious applications.

Question	Please indicate which most applies to your organisation	*If you have a plan for putting this control in place, when?* 6mth	12mth	24mth	24mth+	**Comments** (including any reasons the recommended control is not applicable to your organisation)
8. Is data on all your devices regularly backed-up? (e.g. to cloud-based service or external hard drive)	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
9. Are all sensitive documents encrypted before you send them over the internet? (e.g. email, file sharing service)	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
10. Do you have up-to-date firewall[6] protection for any systems or devices connected to the internet?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
11. Do you use a proxy / web filtering[7] service to automatically scan and allow or block access to certain websites on all your devices?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
12. Do you restrict application usage[8] to prevent untrusted applications from running on your devices?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
13. Are unused services and ports on all your devices disabled[9]?	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
14. Is autorun[10] disabled on all your USB drives?	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
15. Do you have a guest network[11] available on your Wi-Fi for customers/clients?	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	

6 **Firewall** is hardware or software that monitors incoming and outgoing network traffic (for example to or from the internet) and permit or blocks traffic based on a set of security rules. Firewalls can block suspicious traffic and prevent attacks.

7 **Proxy/web filtering service** is a service that sits between you and the internet. It runs every website request through a filter, looks up each address in its database of allowed or disallowed sites, and allows or blocks each request accordingly. This can be used to ensure websites with bad reputations are automatically denied if requested by users.

8 **Restricting application usage** is restricting the ability of software programmes and processes able to run on a device to a list of known and trusted applications. Usually carried out by policies and rules on the device's operating system or by software installed on the device. Further guidance on **https://www.cyber.gov.au/publications/implementing-application-whitelisting**

9 **Disabled ports** are services or protocols not required for systems to function made inoperable.

10 **AutoRun** is the ability of programmes or services to be automatically launched from a USB drive as soon as it is plugged into a device. You can search the USB manufacturer's support pages for guidance on disabling autorun.

11 **Guest network** is a network (usually Wi-Fi) provided for external parties (e.g. clients) that is segregated from networks used by the business, preventing third-party access to information held by the business.

Question	Please indicate which most applies to your organisation	*If you have a plan for putting this control in place, when?* 6mth	12mth	24mth	24mth+	**Comments** (including any reasons the recommended control is not applicable to your organisation)
16. If you have a website(s) – Do you regularly engage a security consultant to independently test your website for vulnerabilities? (i.e. penetration testing[12])	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	

Section 3: Ensuring information is only being accessed on a need to know basis, and regularly reviewing who can access what information.

Question	Please indicate which most applies to your organisation	*If you have a plan for putting this control in place, when?* 6mth	12mth	24mth	24mth+	**Comments** (including any reasons the recommended control is not applicable to your organisation)
17. Do you use multifactor authentication[13] for any online service containing personal information? (e.g. your email accounts, case management system)	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
18. Have you ensured default credentials[14] (factory setting passwords) on any off the shelf product you use have been replaced with strong passwords? (e.g. new software, network devices and web services)	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
19. Do you regularly review user and administrator accounts and disable accounts you no longer require?	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
20. Are individual user accounts (not shared) used for logging onto systems and web services?	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
21. Is all information stored and accessed through services and devices under your control? (i.e. not on personal devices of your staff/ volunteers)	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	

12 **Penetration testing** is technical testing by security consultants to find vulnerabilities that could be exploited by malicious parties, using similar tools and techniques as hackers use. Further guidance on **https://www.ncsc.gov.uk/guidance/penetration-testing**

13 Multifactor authentication is a requirement for more than one control factor to be provided in order to gain access to a system. Examples include using an ATM which requires possession of a bank card and knowledge of a PIN number, or one-time code numbers sent to a user's mobile phone once a valid user name and password combination has been provided. CERT NZ has resources on **https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/two-factor-authentication/**

14 Default credentials are any generic username and passwords provided with a system by the manufacturer to allow a new owner initial access to a system. CERT has resources on **https://www.cert.govt.nz/it-specialists/guides/default-credentials/**

Question	Please indicate which most applies to your organisation	*If you have a plan for putting this control in place, when?* 6mth	12mth	24mth	24mth+	**Comments** (including any reasons the recommended control is not applicable to your organisation)
22. **Do your systems require users set strong and difficult to guess passwords?** (For example email passwords have minimum character requirements).	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
23. **Can you monitor and log what information your users have accessed/used?**	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
24. **Do you use a single service to manage the sign-in process (passwords) for multiple applications within your organisation?** (i.e. centralised authentication[15]).	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
25. **Are email accounts within your organisation used for business purposes only?** (i.e. not used to log into Facebook, Twitter, etc)	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	

Section 4: Responding appropriately to a privacy or cyber security incident

Question	Please indicate which most applies to your organisation	*If you have a plan for putting this control in place, when?* 6mth	12mth	24mth	24mth+	**Comments** (including any reasons the recommended control is not applicable to your organisation)
26. **Can you wipe[16] your portable devices remotely if necessary?** (e.g. if a device is lost or stolen)	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
27. **Can you monitor and log any external attempts to gain unauthorised access to your services or devices?** (i.e. monitor attempts to breach firewalls, network devices, database applications, file access on shared drives)	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
28. **Do you have and periodically test processes to restore your IT services following disruption by a significant event?** such as earthquake, fire, flood or other event that prevents your normal operations. (i.e. disaster recovery).	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	

15 Centralised certification is a single service to manage the sign-in process for multiple applications used within an organisation.

16 Remote wiping is the ability to delete all user data and information from a device without being in physical possession of the device. Remote wiping is typically provided on modern smartphones.

Definitions

Table 1: Terms used in these guidelines

Term	Description	More information
Antivirus protection	Antivirus products can detect and block many forms of viruses and other malware hidden in files. Ensuring that all devices (computers, phones, laptops) have antivirus products installed and constantly kept up to date will help to ensure they are adequately protected from malicious files.	**https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product**
Autorun on USB	AutoRun is the ability of programmes or services to be automatically launched from a USB drive as soon as it is plugged into a device.	Search the manufacturer's support pages for your operating system for guidance on disabling autorun.
Centralised authentication	A single service to manage the sign-in process for multiple business applications within a business.	
Cloud-based services	Services delivered by other parties via the public internet to which anyone can sign up or subscribe to use.	**https://www.cert.govt.nz/individuals/guides/stepping-up-your-cyber-security/how-the-cloud-works/**
Court and judicial information	Information that is in the possession of the court and is listed in the District Court Act and that does not fall within the protection of the Privacy Act 2020	*"The Senior Courts Act 2016 Schedule 2 and the District Court Act 2016 Schedule 1 defines categories of court information".*
Default credentials	Any generic username and password provided with a system by the manufacturer to allow a new owner initial access to a system.	**https://www.cert.govt.nz/it-specialists/guides/default-credentials/**
Disabled ports	Computers connect with each other over a combination of services and protocols. Disabled ports refers to the process of making inoperable any service or protocol not required for the system to function.	**https://www.cert.govt.nz/it-specialists/critical-controls/unused-services-and-protocols/**
Disaster recovery	Processes and resources to restore business services following disruption by a significant event such as earthquake, fire, flood or other event that prevents normal business operation.	
Encryption	Encryption is the encoding or 'scrambling' of information so that it cannot be accessed by people who don't have the right key (password) to decrypt it. Encryption can be applied to network traffic, files, folders, portable drives, or entire devices.	Microsoft provides guidance on encrypting files at **https://support.microsoft.com/en-us/help/4026312/windows-10-how-to-encrypt-a-file**.
Firewall protection	A firewall is hardware or software that monitors incoming and outgoing network traffic (for example to or from the internet) and permit or block traffic based on a set of security rules. Firewalls can block suspicious traffic and prevent attacks.	**https://www.staysmartonline.gov.au/protect-your-business/doing-things-safely/firewalls**
Guest networks	A network (usually Wi-Fi) provided for external parties (e.g. clients) that is logically segregated from networks used by the business, preventing third-party access to information held by the business.	
Macros	Macros are small applications that can run inside larger applications – usually within Microsoft Office documents such as Word, Excel and PowerPoint. When used maliciously in a document, macros have the potential to delete files, upload data, or download further malicious applications.	**https://www.cyber.gov.au/publications/microsoft-office-macro-security**

Term	Description	More information
Malware	A kind of malicious software designed to damage or harm a computer system and often aims to go unnoticed.	https://www.cert.govt.nz/individuals/explore/malware/?topic=malware
Multifactor authentication	A requirement for more than one control factor to be provided in order to gain access to a system. Examples include using an ATM which requires possession of a bank card and knowledge of a PIN number, or one-time code numbers sent to a user's mobile phone once a valid user name and password combination has been provided.	https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/two-factor-authentication/
Patch management	The process of ensuring vulnerabilities that have been identified in software or devices are corrected promptly, by installation of security updates released regularly by vendors.	https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/keep-up-with-your-updates/
Penetration testing	Technical testing by security consultants to find vulnerabilities that could be exploited by malicious parties, using similar tools and techniques that hackers use.	https://www.ncsc.gov.uk/guidance/penetration-testing
Personal information	Personal information is any information that could identify a living person. A person doesn't have to be named in the information if they can be identified from it in other ways (for example, by a combination of characteristics, or by association with other information such as the context). Personal information includes contact details, a person's image or a recording of their voice, and their bank account, fines, and financial information.	s7 of the Act, Interpretation and related matters, and s69 Interference with privacy of individual.
Privileged accounts	System accounts that have rights in excess of those required by normal users. Typically used by system administrators for the purposes of managing, configuring or managing access to systems under their control.	https://www.cyber.gov.au/publications/restricting-administrative-privileges
Proxy/web filtering services	A service that sits between you and the internet. It runs every website request through a filter, looks up each address in its database of allowed or disallowed sites, and allows or blocks each request accordingly. This can be used to ensure websites with bad reputations are automatically denied if requested by users.	
Remote wiping	The ability to delete all user data and information from a device without being in physical possession of the device. Remote wiping is typically provided on modern smartphones.	
Restricting application usage	Restricting the ability of software programmes and processes able to run on a device to a list of known and trusted applications. Usually carried out by policies and rules on the device's operating system or by software installed on the device.	https://www.cyber.gov.au/publications/implementing-application-whitelisting
Strong passwords	Techniques to design passwords that are difficult for others to guess, typically involving unpredictable phrases, or the use of multiple character types such as capitalisation, numbers and special characters such as #, ?, <, % etc).	https://www.cert.govt.nz/business/guides/policies-and-processes/password-policy-for-business/
Web services	Services that are provided by other parties via the public internet.	

APPENDIX THREE

Conflict of interest form[17]

Disclosure of possible conflict of interest

Name: **Date of Disclosure:**

I wish to disclose a personal interest that may result in a conflict. I understand a conflict of interest to be a situation where my personal interests compromise, or may be seen to compromise my responsibilities to act fairly and impartially when delivering justice services.

Type of personal interest:

- ◯ Whānau/Relationship
- ◯ Financial
- ◯ Professional
- ◯ Other

Please provide details:

Please answer the following questions:

1. Do you think it is possible that the interest identified above may lead to an unfair outcome and/or inappropriate access to information?
2. Have you already seen or had access to information that could be considered private or sensitive?

I will update this disclosure if my interests change, or if there is a relevant change in circumstances.

I will not access any information related to the case or circumstance that this actual, potential or perceived conflict relates to without prior approval of my manager or my organisation's Board or governance group.

Signed: **Date:**

17 Use of this sample form is not compulsory. Organisations may choose to use their own conflict of interest form.

Management Plan

Assessment of the interest disclosed

Does a conflict exist? ◯ Actual ◯ Potential ◯ Perceived ◯ No Conflict

Comments

Actions taken:

◯ Restricting Involvement

◯ Reallocating Responsibility

◯ Removing the conflict

◯ Relinquishing the work

How this conflict will be managed:

Please answer the following questions:

1. **Has a privacy breach occurred?**

   Note if the answer is Yes, privacy breach procedures must be followed.

2. **Does the Court or Ministry of Justice need to be informed?**

   The Ministry of Justice requires that you document the steps you have taken, and will take, to mitigate any identified conflict of interest as it relates to services that the Ministry funds.

Management plan completed by: **Date:**

Agreed to by the person with a conflict: **Date:**

Review by Organisation's governance group (if applicable) **Date:**

PHONE: **+64 4 918 8800**

FAX: **+64 4 918 8820**

EMAIL: **info@justice.govt.nz**

WEB: **justice.govt.nz**

IBSN: 978-0-473-54907-7 (PDF)

Published by:

Ministry of Justice
DX Box SX10088
Wellington
New Zealand

September 2020

New Zealand Government

MOJ Ref _ Sept 2020