

An illustration at the top of the page features a stylized owl with large yellow eyes and a red beak, set against a dark blue background with small white stars. To the left of the owl is a glowing red lantern with a yellow flame. The title 'Information Management, Privacy and Security' is written in white text across the middle of this illustration.

Information Management, Privacy and Security

Nau mai, haere mai and welcome

Welcome to the Information Management, Privacy, and Security online training module.

In this module, you will cover:

- what information management is and why it is
- important protecting information
- information privacy and sharing
- how to recognise and report a privacy, information, or IT
- security breach three scenarios
- next steps and where you can find more information.

This module will take you 10-15 minutes. There is audio so please use a set of headphones to not disturb your colleagues.

Introduction

What information management is and why it is important

At MSD, we are kaitiaki of information.


Information that we create or receive as part of our business activities are public records regardless of their format, and are treated and protected as taonga.

All MSD people, including contractors and partners are responsible for managing information through its lifecycle.

Our duty under the Privacy Act 2020 and the Public Records Act 2005 is to safeguard New Zealanders' information. As Ministry staff we all have a part to play in meeting our obligations.

The public expect the Ministry to look after their information. If we don't meet these expectations, we lose the trust and confidence of New Zealanders to deliver our services.

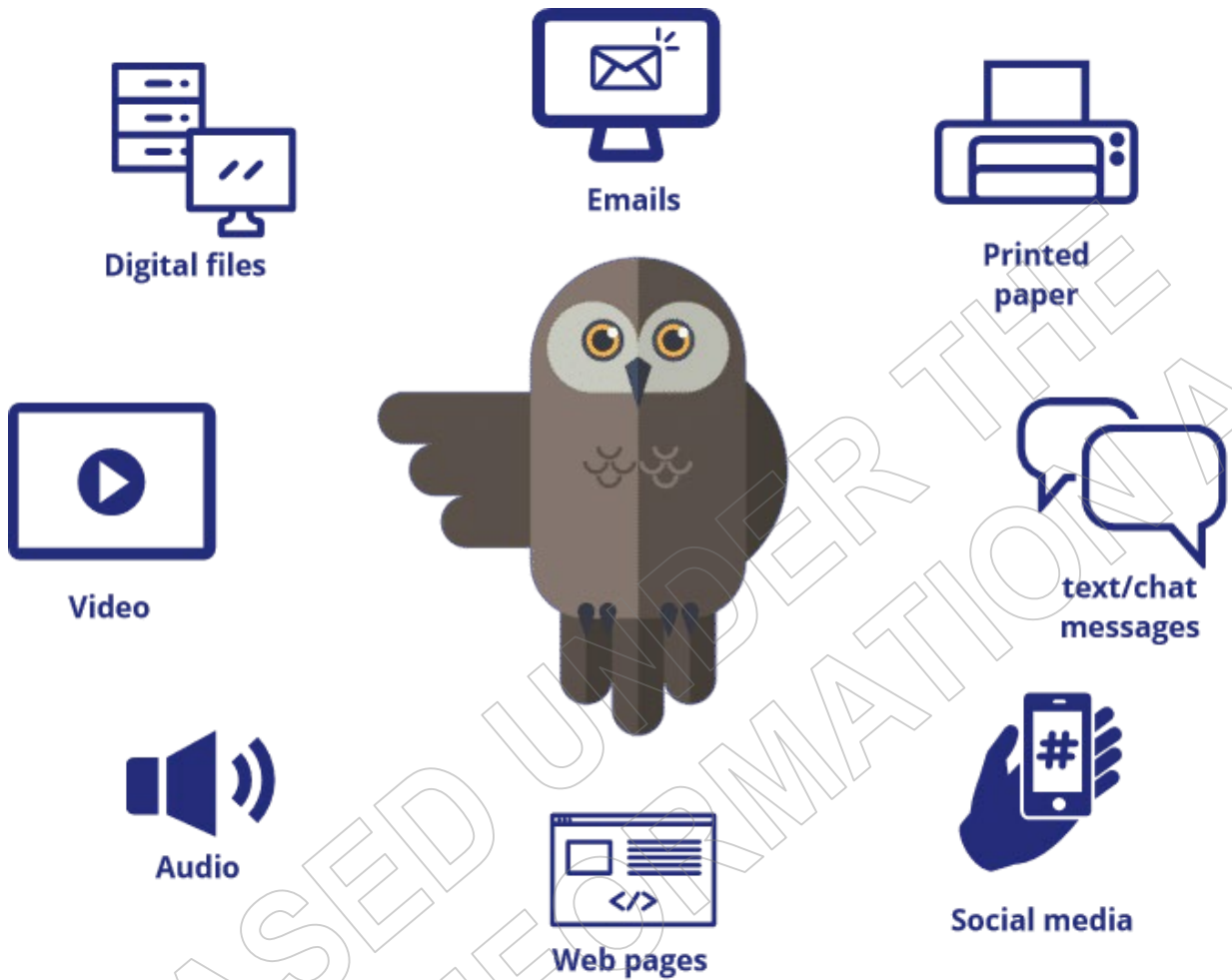
Managing Information



Information is the content that you collect, create, receive, and work with as part of your job.

Information comes in all forms and shapes.

We hold many types of information including information from and about our clients, as well as corporate information that we create and use to manage the business of MSD.



Information management

Information management is about how we create, collect, organise, use, secure, control, share, maintain, and appropriately dispose of this information.



Let's have a look at the information lifecycle and the phases of it.

Saving



You must save information you receive or create which relates to your work on behalf of MSD that provides evidence of our business activities or decisions.

Emails we send and receive that record significant actions or decisions must be stored in the appropriate repository, such as Objective or other line of business systems.

When receiving information from other parties, (e.g. downloaded from the internet or by email), think about the following:

- Check the recipient - do you know this person or were expecting it?
- Don't open unexpected attachments.

For more information on saving, look at this page on [Doogle](#).

Storing



You must only store information in approved MSD information systems, such as Objective or line-of-business systems (e.g. CMS). Avoid keeping it in locations that cannot be accessed by others, such as desktops, hard drives, email inbox or folders, or personal drives.

Digital information is considered the authoritative source and we should avoid keeping paper copies of digital records.

For more information on storing, look at this page on [Doogle](#).

Searching



Information is created and received every day. Making it discoverable and using searches to find relevant information is important. It enables MSD to reuse information and gain insights to deliver better products and services for New Zealanders.

At MSD, a large number of documents are created and saved every day. This is one reason why naming information well is important. Giving your documents meaningful names will make them easier for you and your colleagues to find when you're running searches.

For more information on naming conventions/naming information, look at this page on [Doogle](#).

Sharing



At MSD, access to information must be open by design to all staff, and restricted by exception. This means that information is accessible to all MSD staff and is restricted only where there are legitimate reasons to do so (e.g. personal information). This enables knowledge sharing and reuse of information.

When sharing information with your colleagues, whenever possible, share a link to the original content, rather than sending a copy.

For more information about collaborating and sharing internally, look at this page on [Doogle](#).

When sharing externally, we need to ensure we are protecting

our information, including our clients' rights and privacy, by using an approved sharing mechanism that allows us to share information securely.

For more information about sharing externally, look at this page on [Doogle](#).

Disposing



While we are all responsible for creating and maintaining full and accurate information, it is equally important that we dispose of information when we are legally able to do so.

Different types of records have varying lengths of time they need to be kept before they can be disposed of. This ranges from 'as long as MSD needs it' to 'transfer to Archives for permanent retention'.

Information can only legally be disposed of by the IM team.

The types of information described below have short-term or

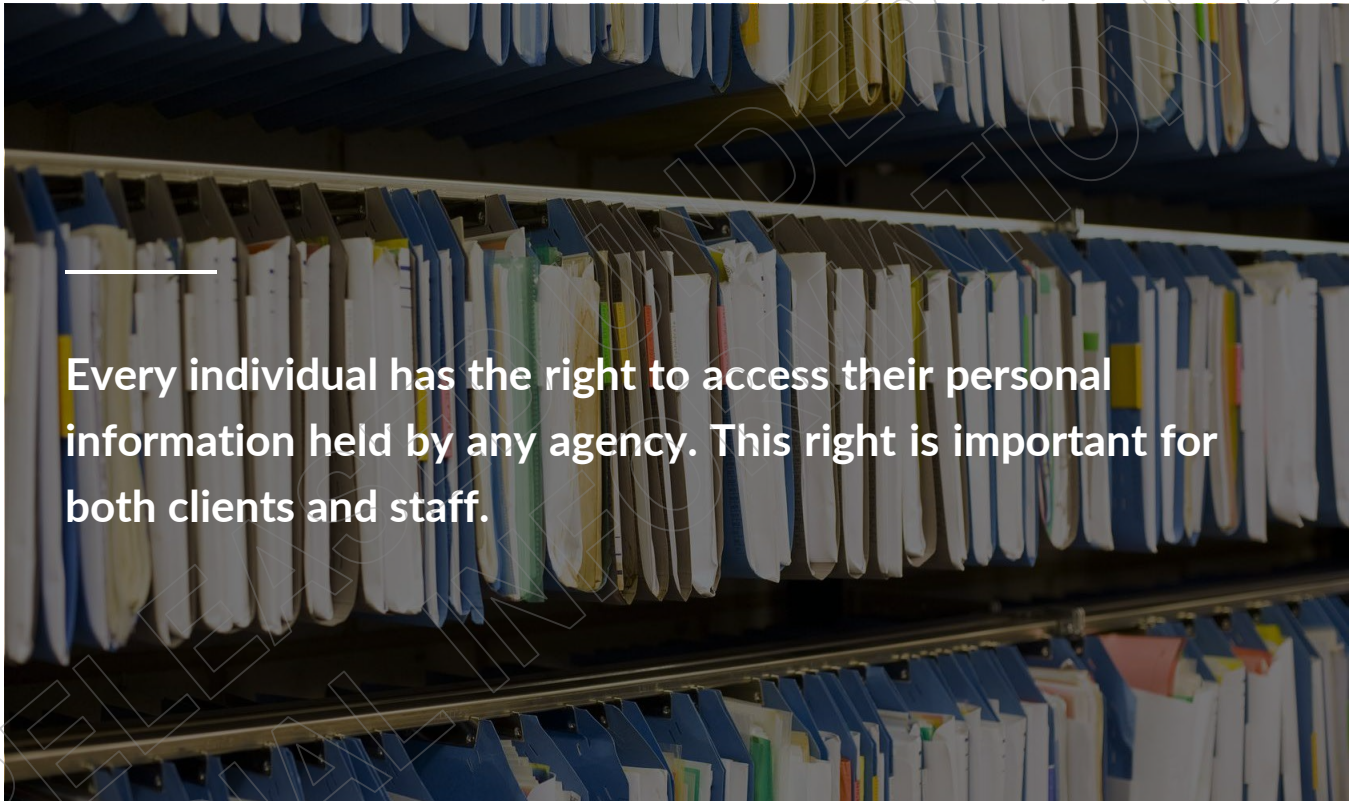
no value and can be deleted by staff when no longer required:

- Short term value - Information that is only needed for a short-term period to support business transactions, decisions or activities, and does not record or add valuable context to them in the long term
- Duplicates - Information that is a duplicate, and a copy has been saved elsewhere in our systems
- No business value - Not business information as it does not provide valuable context to business transactions, decisions or activities.

For more information on disposing, look at this page on [Doogle](#).

You can find more information about managing Ministry information on [Doogle](#), but if you have any questions, contact the [IM team](#).

Rights to access information



Every individual has the right to access their personal information held by any agency. This right is important for both clients and staff.

Providing access is important because it holds us to account about what we do in our roles, how we handle and treat information, and the decisions we make about people.

Providing a client access to the information we hold enhances trust and enables people to query the information we have that might be wrong.

Conversations, emails, notes, opinions, and decisions you make about a person can be requested at any time.

Remember to always be respectful, and keep records professional, relevant, accurate and up to date.

Making a request

A person can make a request for their information in a variety of ways, for example:

- via an email or text direct to a case manager
- via a social media or website channel owned by MSD
- in a written letter
- verbally, over the phone or in person.

Providing access

If we have the information and it's easy to provide immediately, then we should provide it immediately. Usually requests must be acknowledged, and access provided within 20 working days

from the day it was received by the agency or the Ministry. An extension may be granted if the information is difficult to access.

There is no option not to provide access unless specific exceptions or withholding grounds apply. Not providing access to information, could be a breach of the Privacy Act.

Where to find more information

There are clear guides on Doogle on how to handle a request for personal information. Follow the process already established, and if in doubt about what can be released, talk to your manager or a member of the Privacy and Information Sharing team.

Recognising and reporting information breaches

Information breaches can happen for a variety of reasons.

The Ministry has technology to both protect against hackers and prevent accidental information loss. However, hackers or scammers sometimes use sophisticated methods to target individuals in order to obtain information. This along with our often-hectic working lives can lead to things going wrong and a security or privacy breach can happen. We are only human and as humans we all make mistakes. What is important though is how we handle the situation when things do go wrong.

It is really important to contain the impact of an information breach. The number one thing you can do if you think a breach has occurred is to report it to your manager immediately. You will not get in trouble for this.

The Ministry has teams and processes for dealing with breaches and, once notified, these teams will help and support you to manage the breach for the Ministry. Don't worry if you're not sure if you are dealing with a security or privacy breach, the most important thing is to contact your manager who will in turn contact one of the specialist teams and they will work together to contain and resolve any breach.

Examples of a security or privacy breach

- An email sent to an incorrect recipient due to an email address mistype, or out-of-date address held on record, resulting in a loss of control and the disclosure of personal information.
- Losing a physical file containing client or Ministry information in a public place.
- Sending personal information as a result of a phishing attack to an unknown person.
- Scam (phishing) and SPAM emails, phone calls and texts resulting in personal or MSD information being disclosed.

Who to contact

If you think an IT Security breach has occurred, tell your manager who then should contact the **Service Desk** or the **IT Security team** directly for advice or to report the issue.

If you think a Privacy breach has occurred, tell your manager who then should contact the **Privacy Officer** to report the issue.

For more information, look at this **Doogle** page.

Don't worry if you're not sure if you are dealing with a security or privacy breach, the most important thing is to tell your manager.

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Scenario one - Information management

Now we're going to go through a scenario for information management.

Answer the questions below.

1. You have been asked to do a stocktake of supplies in the basement at your work and came across some unsecured boxes of MSD files.

What is the first thing you should do?

- a) Tell the landlord
- b) Close the door and not worry about it
- c) Talk to your manager about what to do.

2. As you go through the files, you find a file that has the same name as your auntie. What do you do?

- a) Have a quick peek inside
- b) Tell your manager so they know there could be a potential conflict of interest
- c) Take photos of the information inside and send them to your auntie

Your manager believes there is not issue as long as you aren't looking inside the files.

After you report back to your manager about the contents, they realise that the files in the boxes need to be registered. This is important so we know what information we hold and where to source them in the future.

3. You register the boxes and send them offsite to the approved storage facility.

Some loose papers and files have been identified as ready for destruction. What do you do?

- a) Dispose of it in the blue destruction bin
- b) Throw it in the big communal waste bin around the corner
- c) Re-use the other side of the paper for taking notes
- d) Create garlands out of them for the Christmas party

4. How would you avoid situations like this in the future? Choose the 2 answers that apply.

- a) Register and store files in an approved offsite storage facility or locked cabinet onsite
- b) Check that it's not already saved somewhere. If it's not, scan it and save it into approved system, then throw away the original paper
- c) Dispose of paper files without an assessment, since the future is digital
- d) Lock the basement and not create a register of the files

Well Done!

Thanks to you, the files are now in a secure and dedicated storage facility and is only able to be accessed by the appropriate authorised personnel via a tracked process.

You can now move on to the next section.

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Scenario two - Privacy

Now we're going to go through a scenario for privacy.

Answer the questions below.

Background

A client called Ami has been disputing entitlement to a supplementary payment. She's made a Privacy Act request for a copy of her whole MSD file. A staff member, Kate, is responsible for acknowledging and managing Ami's request.

Kate knows there's a time restriction to provide the response, so she needs to deal with it quickly.

1. How many days do we have to respond with our decision about whether to provide the information?
 - a) 30 working days
 - b) 20 working days
 - c) 10 working days
2. Kate finds a record that Ami already got a copy of her file 2 years ago. She's not sure whether she has to provide all the information again.

Can Ami ask for her whole MSD file when we have already given her some or all of that information?

- a) Yes - she can ask for any information about herself that MSD holds, even if we have already provided it
- b) No - clients only make repeat requests to cause trouble and we can refuse her request
- c) Yes - but we can check with her whether she really wants everything or only the last 2 years' worth of information
- d) No - she can only ask for the information that we didn't provide before

Kate wants to send an email to Ami acknowledging that MSD has received her request.

At the same time, she is preparing an email to a colleague in MSD who is also called Ami. The email lists all the jobseekers who are due to come to a training course next week, with a variety of information about those jobseekers.

3. Kate sends the email meant for her colleague Ami to her client Ami by mistake. The client is very upset and contacts Kate to let her know what's happened.

What should Kate have done before sending her email? (tick all that apply)

- a) Check the name of the recipient to make sure it's the correct person
- b) Have a cup of tea
- c) Check the contents of the email and any attachments to make sure that information needs to be sent to that person

4. There appears to be some kind of breach – what could the staff member do? (Tick all that apply)
 - a) Report it to their manager
 - b) Complete the Notify a privacy or IT security incident form on Doogle
 - c) Call someone in the Privacy Team or email the Privacy Officer
 - d) Follow the step by step support on Doogle
 - e) Contact the Privacy Commissioner

5. What should Kate say to her client Ami?
 - a) Apologise and make sure that Ami deletes the email
 - b) Try to pacify her and hope the whole thing blows over

6. What could Kate do to reduce the chances of a breach like this happening in future (as well as checking things carefully)?
 - a) Refuse to send any more emails
 - b) Take notice of any STOP, THINK, CHECK popup and switch off auto-complete on her emails
 - c) Nothing - accidents happen all the time

Well Done!

You now have a better idea of what to do to keep information private.
You can now move on to the next section.

Scenario three - Security

Now we're going to go through a scenario for security.

Answer the questions below.

1. You have received an email from an unknown external party. The email asks you to download and open an attached file urgently.

What should you do?

- a) Reply to the sender and ask for further information
- b) Download and open the file
- c) Use the report to Service Desk button in your email
- d) Forward the email home to read it later

2. Later that day you notice your computer is behaving strangely. Windows are opening and closing, and the machine is responding slowly.

What should you do?

- a) Go get a cup of coffee and wait for it to fix itself
- b) Contact Service Desk and let them know
- c) Ask your manager for a new computer
- d) Call a friend who is good with computers for advice

3. The next day you receive a phone call from an unknown number claiming they are trying to fix your computer. They ask for your MSD username and password.

What should you do?

- a) Hang up immediately and ignore the call
- b) Give them your information
- c) Report the call to Service Desk
- d) Transfer the call to your manager

Well Done!

You now have a better idea of what to do to keep information private. You can now move on to the next section.

RELEASED UNDER THE
OFFICIAL INFORMATION ACT

Conclusion and handy links

Congratulations

Well done. You have completed this module on information management, privacy and security.

You have covered:

- what information management is and why it is important
- protecting information
- information privacy and sharing
- how to recognise and report a privacy, information, or IT security breach
- three scenarios.

Main points

The Ministry holds information about people and uses information that impacts their lives. The information we hold and use is **taonga** (a treasure), and as its guardians we must both use it responsibly and protect it while it is in our care.

All MSD staff are responsible for managing information and keeping it safe through its lifecycle.

If you think an information breach has occurred, you must report it to your manager immediately. You will not get in trouble for this.

Every individual has the right to access their personal information held by any agency. This right is important for both clients and staff.



Handy links

The **Information Hub** is a collection of Doogle pages by the Information Group. It has guidance, tools and resources to enable MSD staff to work with information while protecting ourselves, our clients, and our information assets from risk.

Contact Information Management team (infohelp@msd.govt.nz) for advice creating, collecting, organising, controlling, storing, maintaining and disposing of information.

Contact the Privacy Team (PrivacyOfficer@msd.govt.nz) for advice if you think a privacy breach has occurred.

Contact the IT Security Team (IT_Security@msd.govt.nz) for advice if you think a security breach has occurred.

You can now close the module.

RELEASED UNDER THE OFFICIAL INFORMATION ACT