Information Sharing Guidance

Introduction

The purpose of this document is to support agencies to establish or improve information sharing practices. It provides relevant information, high level guidance and key messages to support agencies to make improvements within the current policy settings and operating environment.

All agencies currently share information, between themselves and the public, in many ways.

Information sharing is important. Effective information sharing drives both transparency and public confidence in how public services are delivered and provides agencies with information to deliver better services.

Information sharing is complex and dependent on a range of factors. This guidance is written from a security and classification perspective and should be read in conjunction with the other guidance linked to from this material.

The guidance:

- Describes the context of information sharing between agencies
- Promotes the value of information sharing between agencies and with the public
- Lays out the policy requirements for information sharing in the New Zealand Government Security Classification System
- Lays out key legislative requirements that agencies must abide by when sharing information, and references tools and mechanisms that can be used by agencies to enable information sharing

Application

This guidance applies to all government information, regardless of form or format, including speech, documents, and data that the New Zealand government collects, stores, processes, generates, or shares to deliver services and conduct business.

Where do I go for more information?

The following shows where to go for more information on a range of information sharing questions:

1. **What information can I disclose following a request for official information made under the Official Information Act?**

   https://www.ombudsman.parliament.nz/agency-assistance

2. **What information can I disclose following a request for official information made under the Local Government Official Information and Meetings Act?**

   https://www.ombudsman.parliament.nz/sites/default/files/2019-08/The%20LGOIMA%20for%20agencies%20August%202019.pdf

3. **What information can I release following a request for personal information made under the Privacy Act?**

   https://www.privacy.org.nz/privacy-act-2020/privacy-principles/

4. **How should an agency proactively release official information to the public?**

   https://www.ombudsman.parliament.nz/sites/default/files/2021-12/Proactive_release_December_2020.pdf

   https://dpmc.govt.nz/publications/co-18-4-proactive-release-cabinet-material-updated-requirements

   https://www.publicservice.govt.nz/our-work/official-information/

   https://www.publicservice.govt.nz/assets/SSC-Site-Assets/Proactive-Releases/Cabinet-paper-The-Next-Steps-in-the-Public-Release-of-Official-Information.pdf

5. **How should an agency proactively release historical records that are of interest to the public?**

   https://protectivesecurity.govt.nz/classification-system/how-to-declassify

6. **How do I know if I need some sort of official agreement to share information, e.g., an Approved Information Sharing Agreement (AISA)?**

   https://www.privacy.org.nz/assets/New-order/Privacy-Act-2020/Information-sharing/Approved-Information-Sharing-Agreements/Approved-Information-Sharing-Agreement-guidance-March-2015.pdf

7. **How should my organisation manage the ongoing disposal of its records, including deciding which records are of long-term value and will be transferred to Archives New Zealand?**

   https://www.archives.govt.nz/manage-information

8. **Where do I go if I am uncertain about what to do with classified information?**

   For general instructions about how to classify and handle classified information:

   https://protectivesecurity.govt.nz/classification-system

   For information about technical requirements:

   https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/

9. **Where do I go for information about data systems?**

   For information about using data systems to enable secure access to data:

   https://swa.govt.nz/what-we-do/data-systems/

10. **Where do I go for information about data policy?**

    For information about the Data Protection and Use Policy:

    https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/data-protection-and-use-policy-dpup/

Why is information shared?

Information is shared for a variety of reasons and these affect what type of and how much information should be shared.

Information sharing can improve public services

All agencies require information to make decisions and direct their services. This is as true for agencies delivering infrastructure as it is for those delivering services. Information provides the evidence to direct agency outputs, from building new schools to resourcing social services.

Effective and appropriate information sharing is important as the information needed for an agency to make robust decisions is often held across numerous / different organisations.

In most cases, this can be achieved with aggregated and de-identified information.

Appropriate information sharing supports democratic values

Transparency and open government are key issues for democracies. This means that over and above the operational value of sharing information, agencies need to view transparency as a public good.

New Zealand has one of the most trusted public sectors in the world. Appropriate information sharing is a key element of transparent and effective

government, and all agencies have a role to play in maintaining and promoting access to government information.

Information of this nature is usually shared as a result of either an official request under legislation or through proactive release by the agency.

Better information sharing can improve the safety and security of New Zealand and New Zealanders

Information sharing has particular importance for those agencies responsible for public safety and national security issues.

Information sharing has many potential benefits and, in the right circumstances, could prevent loss of life. Equally, information sharing on security matters presents challenges, especially relating to the obligations and practices associated with handling more highly classified information

Information of this nature is shared both through established arrangements between agencies and case-by-case sharing as a response to specific incidents.

What does successful sharing of information look like?

Success means that information is shared when it can be and protected where it needs to be. Sharing information provides agencies with necessary information through which better public services are delivered. Protecting information means that harm does not result from information being shared inappropriately.

Successful information sharing means that information is shared proactively and reactively through well planned arrangements and supported, where necessary, by formal agreements. This includes system to system data feeds as well as contact from one agency to another on specific and sensitive matters.

Not all information can or should be shared. All agencies have responsibilities to protect personal information. In addition, agencies working in public safety and national security may face additional requirements to protect information. For example, more highly classified information can only be shared with organisations that have appropriate systems in place. In addition, some agencies may hold information that they are not allowed to share without the permission of the agency that gave it to them (known as 'originator controlled').

Success means agencies can interpret the need-to-know principle

The Protective Security Requirements state that 'only people with a proven need-to-know should be granted access to official information'.

Need-to-know refers to a 'need to access information based on an operational requirement'. In plain English, if someone needs a piece of information to do their job, they have a need-to-know.

However, for several reasons, this does not always mean that they can be given the information.

The application of the need-to-know principle is sometimes an impediment to information sharing and the principle is discussed in more detail later.

Success means that agencies proactively look to share information when it would add value to do so

As described above, there are clear reasons why some information should not be shared. However, a repeated criticism is that these reasons are over-extended, i.e., used to prevent information sharing unnecessarily and unjustifiably.

Collectively, the public service holds large amounts of information that – when appropriately shared – provides insights and informs better services for New Zealand and New Zealanders. If this information is not shared with people who can use it, then it creates no value.

Agencies are recommended to take a trust-based approach to information sharing. While need-to-know requirements need to be satisfied, they should not be over-extended.

Success means that agencies only share information that is necessary

While sharing information can create value, sharing too much information can also increase risk and cause problems. Sharing more information than necessary makes it more difficult to find and act on the right information. Any information that is shared must also be stored and secured. The more information that is shared, the greater the burden on the agency receiving the information and the greater the risk of that information being inadvertently disclosed.

Success means that agencies consider whether they can achieve information sharing objectives without releasing personal information

Information sharing should occur to support specific outcomes, e.g., for an agency to deliver a particular service. Agencies should consider whether these objectives can be met without sharing personal information. Further, if personal information is required, can the same objectives be met if data was anonymized.

The underlying principle is that agencies should only share information which is necessary. For example, a health agency might need and request information on the numbers of people receiving a certain treatment and how it was delivered. This information may be held on a database containing personal information about the individuals concerned. In this case, the personal information is irrelevant to the request and would need to be removed if the database was to be shared.

How is information shared?

Information sharing can occur in many ways, e.g., with other public sector agencies, private sector organisations, governments, groups, and/or members of the public.

The picture below provides a simple summary of the main ways through which information is shared and the key legislation involved.

Sharing information as required by legislation

The NZ Government Classification System Policy says, "Agencies must understand their information sharing obligations under relevant legislation (e.g., Privacy Act), and regulatory or partner agreements that enable and hinder information sharing across partners."

To achieve this, organisations need to ensure that their people understand their obligations to share information and can do so, e.g., have the appropriate training and delegations.

While it is not always obvious how valuable a single piece of information is, agencies should ensure no one feels they might be sanctioned for sharing information that they have reasonable grounds to think could prevent harm.

In general, wherever there is a threat to life or safety information can be shared. Agencies should have policies and procedures in place in the event that information needs to be shared in these circumstances.

Sharing information under the Privacy Act

The Privacy Act 2020 provides the rules in New Zealand for protecting personal information and puts responsibilities on agencies and organizations about how they must do that. The Privacy Act governs how organisations and businesses can collect, store, use and share personal information.

There are two main types of Privacy Act requests.

- Individuals, or agents acting on their behalf, can request information that is held about themselves (requests under Privacy Principle 6)
- Anyone (individuals and organisations) can request an agency or organisation to disclose personal information if they believe that the reasons for disclosure are consistent with the exceptions described in the Act.

Whenever information sharing agreements are defined in legislation, these have precedence. **Where another law says you should provide information, you are always able to do so**

Information may also have additional, specific requirements about how it can be managed. For example, health information must be managed according to the Health Information Privacy Code. Further information is available from the Privacy Commissioner[4].

Sharing information under the Official Information Act

The OIA allows New Zealanders to have access to information that enables their participation in government and hold governments and government agencies to account.

The OIA allows New Zealand citizens, permanent residents, and anyone who is in New Zealand to request any official information held by government agencies

The principle of availability underpins the whole of the OIA. The OIA explicitly states that:

> *'The question whether any official information is to be made available … shall be determined, except where this Act otherwise expressly requires, in accordance with the purposes of this Act and the principle that the information shall be made available unless there is good reason for withholding it (emphasis added)'.*

The OIA aims to increase the availability of official information (i.e., information held by a government agency) to New Zealanders. Under the Official Information Act information must be made available if requested unless a reason exists under the Act for refusing it.

While the OIA does not provide a mechanism for information sharing across Government, its principles provide a common reference point to make decisions about information sharing.

Further guidance is available from the Ombudsman.

Sharing information under the Public Records Act (PRA)

The purpose of the Public Records Act includes 'the preservation of, and public access to, records of long-term value'.

Records may be 'open access' (in which case they are available to the public) or 'restricted access'. Section 43 of the PRA requires the chief executive to categorize all public records in existence for 25 years as either open access or restricted access. Section 44 of the PRA specifies that decisions about access must be made based on whether there are good reasons to restrict public access or if other legislation which requires the records to be restricted.

When determining whether information and records should be 'open' or 'restricted', organisations should always begin with an assumption of openness unless there are good reasons to restrict. The PRA covers a range of reasons why access should be restricted including national security and international relations and preventing the disclosure of highly sensitive personal information. Without such reasons, records should be 'open access'. Additionally, in specific circumstances, agencies may choose to allow special access to restricted records.

The PRA governs the release of archived information and is not primarily a mechanism for information sharing as described in this guidance. Further information is available from the Chief Archivist.

Other aligned legislation and policy

Agencies should understand all legislative requirements they have regarding information sharing, for example by identifying and capturing any legislation and policy that has a specific information sharing requirement. For example, the Department of Corrections lists all of its information sharing obligations on its website[1].

General expectations of information sharing are set out in the Declaration on Open and Transparent Government[2] through which 'the [New Zealand] government commits to actively releasing high value public data'.

[1] https://www.corrections.govt.nz/resources/policy_and_legislation/Prison-Operations-Manual/Communication/C-10-Official-information-disclosure/C.10.03-Information-sharing-with-other-government-agencies

[2] https://www.data.govt.nz/toolkit/policies/declaration-on-open-and-transparent-government/

Protective Security Requirements (PSR)

The PSR is New Zealand's best practice security policy framework. It sets out government expectations for managing personnel, physical and information security. It details mandatory information security requirements and specific protective security measures to manage the NZ Government Security Classification System and the use, handling, management, and storage of classified material. It is supported by the New Zealand Information Security Manual (NZISM) that is the technical authority for technology systems managing government information.

The PSR defines the security classification system for national security information and information received from foreign governments. NZ Government must adhere to any provisions concerning the security of such information referenced in multilateral or bilateral agreements and arrangements to which NZ or an organisation is party. Release of information requires written approval from the relevant foreign government. Further information is available from the PSR website[3].

Proactive information sharing

Under the Public Records Act, information of long-term value will become available at a determined point in time. Proactive release of information takes place when agencies choose to release information before that date. This usually happens through the following mechanisms.

Proactive release of government information

This includes the release of government information without any request from the public. Government has set expectations that all agencies take a more proactive approach to releasing government information[4]. For example, this has included guidance on publishing completed OIA requests and strengthening the proactive release of cabinet papers[5].

Declassification of highly classified records

Few agencies hold substantial highly classified records. Under the NZ Classification System Policy, such agencies are required to have a policy to lay out how they intend to approach the proactive declassification of this material.

The intent of a declassification programme would normally be to release information to the public, i.e., so that it is now unclassified. The principles of the OIA provide clear guidance on whether information would be releasable.

[3] https://protectivesecurity.govt.nz/

[4] Acting in the spirit of service: official information. Proactive release of official information. *State Services Commission (2018)*

[5] Cabinet Paper: strengthening proactive release requirements *(September 2018)*

Guidance for agencies on how to set up a declassification programme is available on the PSR website: How to declassify information.

Reclassification of classified information to enable better information sharing

When information is highly classified and cannot be shared, agencies should think about whether material can be rewritten at a lower classification level to enable information sharing.

Sharing information in these ways requires consideration of how the information is moved, i.e., from a higher classified system to a lower classified system; and who it will be seen by, i.e., between security clearance holder levels and non-security clearance holders. Agencies must ensure that information is moved appropriately and stored where it will only be seen by those who have a need to access the information.

The use of formal information sharing agreements

Agencies share information through informal and formal mechanisms. Agencies do not need formal mechanisms to share information within the bounds of the OIA, Privacy Act and other legislation.

Information sharing can take place through, or be facilitated by, the following mechanisms:

1. *Formal Information sharing under legislation includes Approved Information Sharing Agreements (AISAs).* AISAs are formal agreements created under the Privacy Act that allows personal information to be shared between agencies for the purpose of delivering public services. AISAs can authorise information sharing arrangements which grant exemptions to some of the Information Privacy Principles.
2. *Agencies may also have memorandums of understanding (MoU) to support information sharing*. MoUs do not give any legal authority to share information but do record organisational commitments to, and arrangements for, sharing information.
3. *Information sharing between agencies.* This can range from staff from different agencies working together on a joint initiative to an individual asking a colleague in another agency to share a document with them. Where an AISA or MOU is not in place, sharing or releasing of information should follow the principles of the Privacy Act and the OIA.

Do I have to have an approved agreement in place to share information?

No. AISAs can improve the extent of information sharing and make it happen more efficiently. Where agencies repeatedly share information with each other, formal agreements can be important to set down the purpose for the information being shared and potentially to make information sharing arrangements more efficient.

Opportunities

Leveraging technology to access data

Information sharing is still often seen as one agency sending information to another, e.g., by manually sending out data. Such approaches are potentially slow and do not take advantage of readily available technologies.

Some agencies are now considering information access rather than information movement, e.g., by providing ongoing access to systems rather than responding to one-off requests. This provides scalable and repeatable access to information by providing secure access to agreed types of information.

The potential access to greater volumes of data and personal information requires commensurate attention to how access to such information is controlled.

Stewardship not ownership

Statistics New Zealand has established a Data Stewardship Framework for New Zealand. Stewardship is a useful concept to enable data sharing as it considers both the ownership and the use of data. For the most part, agencies do not own data but rather they hold data about New Zealanders on their behalf.

When used securely and with New Zealand's trust, data should be seen as a means to provide rich insights, inform decision making and innovation and thereby improve services for New Zealanders.

Assessing the need to share information

Before agencies share information, they should know who they should share it with and for what purpose.

Information sharing most often occurs between relatively small clusters of agencies who have information sharing agreements that reflect shared operational priorities. For example, the Ministry of Justice, Ministry of Health, Oranga Tamariki and other agencies share information to better enable the safety and wellbeing of children and young people in care[6].

Such arrangements are obviously important and of value. Agencies are also encouraged to consider whether there are broader opportunities to share information with agencies not currently considered today.

6 https://www.justice.govt.nz/justice-sector-policy/key-initiatives/addressing-family-violence-and-sexual-violence/a-new-family-violence-act/information-sharing-guidance/

To do so, agencies should first assess the adequacy of existing information sharing arrangements. This could involve the following steps:

1. Identify what information you hold and how, when and for what purpose is it collected and used
2. Identify if there is further information that would enable the agency to deliver its services better
3. Confirm whether the nature and purpose of any new information sharing is permissible (under legislation and relevant policies)
4. Do existing arrangements support any changes to information sharing? If not, how do they need to be changed?

Effective information sharing should flow in two directions. Agencies may receive information from other agencies in order to deliver their own services most effectively. Conversely, agencies may need to provide information to other agencies.

This intent faces a practical difficulty that agencies may not know what information other agencies hold and whether they have an operational requirement (need-to-know) for it.

It is highly recommended that agencies carry out the proposed steps in consultation with those agencies they work alongside. This will enable agencies to 'know what they don't know' about what information is available and facilitate a conversation about whether there is a need-to-know.

Periodic reviews of information sharing requirements and agreement should be undertaken to identify if opportunities exist for further information sharing and to ensure existing arrangements are still fit for purpose. These reviews should include input from staff with operational as well as policy roles, and keep in mind policy and legal considerations.

Which agencies can drive changes to information sharing?

All agencies have a responsibility to consider their information sharing arrangements. However, individual agencies may lack the authority or leverage to influence wider information sharing.

Lead agencies (i.e., with sector or multi-agency responsibilities) are better positioned to determine whether information sharing can be improved in their areas of accountability. If it is not, they should drive the development of any agreements necessary to improve and broaden information sharing.

Removing barriers to information sharing

Barriers

There are a number of barriers to information sharing. This section identifies a range of key barriers and provides some guidance on how to reduce these. It is acknowledged that some barriers, especially those concerning systems, may not be resolvable in the short-term. Where possible, some guidance is provided on how agencies can work within these constraints.

Systems barriers

Systems barriers exist when technology prevents or restricts information sharing. For example, SENSITIVE or RESTRICTED information require emails to be encrypted and sent and received on a system that is accredited by GCSB to provide an appropriate level of encryption, such as SEEMail.

In addition, some agencies may take different approach to technology which makes it harder for them to share information. For example, one agency may want to share information between systems (e.g., by using APIs) and protected by encryption, while another may want to receive information on a USB drive.

Process and behavioural barriers

Information sharing requires clear process and delegations. People may want to share information but not do so if they are unsure about how to do so.

Overlaying this, people are often busy in the workplace and may take shortcuts to save time. In some agencies, this can lead to automatic over-classification information rather than conscious assessment. This is even more likely if people are not confident about what they should do.

Cultural barriers

In some agencies, organisational culture can hinder information sharing, especially where people are concerned about what might happen to them if information is inadvertently released. This is not limited to the national security sector and requirements to manage highly classified information. Privacy breaches can have a serious impact on all organisations.

Information sharing objectives

Enabling information sharing requires barriers to be mitigated at many different levels. This section provides some information sharing objectives and supporting actions.

At an organisational level, agencies need to understand what information they hold for what purpose and to understand their information sharing obligations. To make improvement, agencies need to evaluate [ideally with other agencies] opportunities to improve services through more effective information sharing. This requires:

- Information sharing agreements to be in place [if necessary].

At a people level, people need-to-know who to share information with and how to share it. This requires:

- Clear operational procedures and delegations for information sharing
- Staff to be confident in applying these procedures, e.g., by having received suitable training
- Staff to recognise the value of information sharing.

At a cultural level, organisations need to have a culture that actively promotes information sharing. This requires:

- Policies that reinforce the value of information sharing
- Aligned communications and leadership from the executive down that promotes information sharing

It is naïve to assume that policy and communications are sufficient to drive change. The lived experience for some people working in government is that they continue to feel that if they make a mistake with information sharing, it could be career-limiting or even employment-ending.

Agencies need to promote both the value of sharing and the value of protecting information. As much as there is a cost to inappropriately releasing information, there is a cost to inappropriately protecting it.

An effective information sharing culture does not over-emphasise either sharing or protection at the expense of the other. Rather, it enables staff to make appropriate decisions when they share information and supports them when they have done so.

Applying the need-to-know principle

Only people with a proven need-to-know should be granted access to official information.

The principle applies regardless of the classification level of the information and the seniority or position of the person asking for information. For example, medical staff have no need to look at a patient's medical records if they are not involved in their treatment.

Need-to-know 'refers to a need to access information based on an operational requirement'. In plain English, if someone needs a piece of information to do their job, they have a need-to-know.

This does not always mean that information can be released, and need-to-know requirements must be considered alongside the following factors:

1. Am I allowed to release the information? An agency may hold originator-controlled information which it either cannot release or must seek the permission of the originator before doing so.
2. Is the person asking for the information allowed to receive it? For some information, a security clearance is required to view the information. In a commercial setting, it might mean confirming a contractor has signed a non-disclosure agreement before sharing business information. Equally, some information can only be shared subject to certain controls, e.g., must be shared on an accredited IT system.
3. Consider if the information could be shared in an anonymised or de-identified format, if the proposed data contains personal information
4. Consider if there are any other reasons why the information may not be shareable, for example if a Confidentiality Agreement exists.

These questions are not about need-to-know but they may prevent information from being shared.

How do I decide if there is a 'need-to-know?'

Agencies holding information still maintain a responsibility to check whether information should be shared, including confirming that there is a need-to-know.

Within an agency this can be straightforward as need-to-know may be managed by access control. For example, files about some issues may only be accessible to those staff working on them.

It is harder to assess whether someone from an external agency has a need-to-know. The receiver of a request for information may not have much knowledge of the other agency's operations and be unable to assess whether the requestor has an 'operational requirement' or not.

The guidance recommends that a trust-based approach is used between agencies. Agencies must take a strict approach to handling instructions, e.g., confirming if the recipient of classified information is suitably cleared.

Information Sharing case study

Note: this example is illustrative only.

The Chief Executive of a Government Agency is given a highly classified briefing on a potential terrorist threat to their organisation's staff. The briefing contains a number of signs and suspicious behaviours that their staff should be on the lookout for. Their organisation has limited (or no) capability to handle highly classified information and it is therefore not able to be shared.

In this instance, their staff do not have the security clearances and systems required to receive highly classified information and there is no way to pass the information on.

However, the originators of the information could have been more flexible in how things were classified. For example:

Does the most highly classified information need to be in the briefing at all? If the intent of the information is to inform agencies of a threat and advise them of what they should do, is inclusion of highly classified information necessary? For instance, information about how the intelligence services came about information may need to be highly classified but is not needed to meet the intent of the briefing.

Can the briefing be classified by paragraph? If a document is classified as a whole, then the entire document is necessarily classified at the level of the most highly classified piece of information, even if most of the remaining content would be classified much lower. Classification by paragraph makes it much easier to identify and share parts of a document.

When creating a document, it is important to consider the audience and what the objective of that document is. Can the objective be met by providing information that the audience is able to use?