1 December 2023

[redacted]

Dear [redacted]

Thank you for your Official Information Act 1982 (OIA) request, received on 4 November 2023. You requested the following:

1. *(…) under sec 22 of the oi act i request hard copies of all documents containing policies, principles, rules and guidelines about ird internal policy about , first, the oi act and official information . second internal ird rules about privacy act 2020 and privacy (…).*

On 4 November 2023, Inland Revenue received a follow up email, requesting the following:

2. *"(…) under sec 12 of the oi act i request which group in ird handles formal complaints about NON tax matters (…) the name of its lead manager (…) e-mail address for such complaints (…).*

Item 1

I am releasing in full, attached as **Appendices A** to **E,** respectively, Inland Revenue's *Guide to Official Information Act and Privacy Act Requests,* the summary of the GMS' *Official Information Act 1982 training guide*, Inland Revenue's guide to the publication of responses to requests for Official Information, GMS's *OIA basics* guide, and GMS' guide to *Managing an OIA request*.

I am releasing in full, attached as **Appendices F** to **H**, respectively, GMS' *Day-by-day OIA process*, Inland Revenue's guide to releasing the names of its staff in response to information requests, and Inland Revenue's guide to *Managing Personally Identifiable Information* with some information excluded as it falls outside of the scope of your request.

I am partially releasing, attached as **Appendix I**, Inland Revenue's internal publications on OIA requests with some information excluded as it falls outside of the scope of your request and some information withheld under section 9(2)(a) of the OIA, to protect the privacy of natural persons.

I am partially releasing, attached as **Appendix J**, Inland Revenue's internal publications on the Privacy Act 2020 and privacy related matters with some information excluded as it falls outside of the scope of your request and some information withheld under section 52(3)(b)(i) of the OIA and section 18(3) of the Tax Administration Act 1994 (TAA) as the release of the information would adversely affect the integrity of the tax system or would prejudice the maintenance of the law.

I am withholding two documents in full under section 52(3)(b)(i) of the OIA and section 18(3) of the TAA, as the release of the information would adversely affect the integrity of the tax system or would prejudice the maintenance of the law.

Inland Revenue's *Official Information Requests guide* and the Governance, Ministerial & Executive Services team's *Official Information Act 1982 training guide* are not attached as

they were released to you on 2 May 2023 and 21 August 2023, respectively, as part of the responses to your previous OIA requests.

Item 2

Inland Revenue does not have a team that handles non-tax related complaints exclusively. Complaints at Inland Revenue are handled by the Complaints Management Service team (complaints team), led by Anne Apineru. You can reach the complaints team at complaintsmanagementservice@ird.govt.nz.

Public interest considerations

As is required by section 9(1) of the OIA, I have considered whether the grounds for withholding the information required are outweighed by other public interest considerations which would make it desirable to make this information available. In this instance, I do not consider that to be the case.

Right of Review

If you disagree with my decision on your OIA request, you can ask an Inland Revenue review officer to review my decision. To ask for an internal review, please email the Commissioner of Inland Revenue at: commissionerscorrespondence@ird.govt.nz.

Alternatively, under section 28(3) of the OIA, you have the right to seek an investigation and review by the Ombudsman of my response to your request. Information about how to make a complaint is available at www.ombudsman.parliament.nz or via freephone on 0800 802 602. Alternatively, you can email info@ombudsman.parliament.govt.nz.

If you choose to have an internal review, you can still ask the Ombudsman for a review.

Publishing of OIA response

We intend to publish our response to your request on Inland Revenue's website (ird.got.nz) as this information may be of interest to other members of the public. This letter, with your personal details removed, will be published in its entirety. Publishing responses increases the availability of information to the public and is consistent with the OIA's purpose of enabling more effective participation in the making and administration of laws and policies and promoting the accountability of Ministers and officials.

Thank you again for your request.

Yours sincerely

Josh Green
Domain Lead, Governance and Ministerial Services

Inland Revenue
Te Tari Taake

Guide to
Official Information Act
and
Privacy Act requests

Contents

Introduction

Information is fundamental to the operation of Inland Revenue and is found in many forms, including taxpayer specific information, internal policies and employee information. All information obtained by Inland Revenue must be held in the upmost trust. Consideration must be given to the concepts of confidentiality and privacy when dealing with any information.

Inland Revenue is subject to the Tax Administration Act 1994 (TAA), Official Information Act 1982 (OIA) and Privacy Act 2020 (PA). These Acts impose requirements on how we deal with requests for information.

The purpose of the OIA is to facilitate open government, and therefore the presumption is Government agencies will be as open as possible. Likewise, the PA gives individuals a right to access personal information about themselves that is held by an agency.

The Commissioner of Inland Revenue has an obligation under the TAA to maintain confidentiality in relation to sensitive revenue information and is not required to disclose information that would adversely affect the integrity of the tax system or the maintenance of the law. The general right of access under the OIA and the individual's right to personal information under the PA are both subject to these provisions. Therefore, it is important to understand the inter-relationship between the TAA and the OIA or PA.

This guide is designed to assist people to recognise and respond to requests for official information. This guide is based on a guide produced by the Ombudsman for requests made under the OIA and PA. This guide also explains the process to determine whether requests for information fall within the confidentiality provisions in the TAA.

Although case study examples are included in this guide, requests for official information must be assessed on a case-by-case basis under the relevant Acts (the TAA, OIA and/or PA) when deciding to release or withhold information. Decisions to release information must be made by those with the appropriate revenue delegation or approval authority.

What is official information?

All information held by Inland Revenue is **official information.**

Official information is not limited to documentary material. It includes material held in **any format**, such as:

- **Written documents** including reports, memoranda, letters, notes, emails, eCase notes and attachments—even text messages and draft documents.
- **Non-written documentary information** such as material stored on or generated by computers, including databases, storage devices e.g. iron–keys, video or audio recordings.
- **Information that is known to Inland Revenue**, but which has not yet been recorded in writing or otherwise (including knowledge of a particular matter held by an officer, employee or member of Inland Revenue in their official capacity).
- **Documents and manuals** that set out the policies, principles, rules or guidelines for decision-making by Inland Revenue.
- **The reasons for any decisions** that have been made about a person.

What is not official information?

Official information does not include:

- Library or museum material for reference or exhibition purposes.
- Information held by an agency solely as an agent or for the sole purpose of safe custody on behalf of a person who is not subject to the OIA.
- Information held by the Public Trustee or Māori Trustee in their capacity as a trustee.
- Evidence or submissions to a Royal Commission or a commission of inquiry.
- Certain information relating to inquiries established under the Inquiries Act 2013 (evidence or submissions subject to an order forbidding publication, and documents relating to the internal deliberations of an inquiry).
- Any correspondence or communication between any agency and the Ombudsman or the Privacy Commissioner, in relation to their investigations.
- Victim impact statements.
- Evidence, submissions or information given or made to the Judicial Conduct Commissioner, a Judicial Conduct Panel, or the Judicial Complaints Lay Observer.

Is the information 'held' by Inland Revenue?

It doesn't matter where the information originated, or where it is currently located, as long as it is held by Inland Revenue. For example, the information could have been created by a third party and sent to Inland Revenue. The information could be held in the memory of an employee of Inland Revenue.

For the OIA to apply, the information must be held by Inland Revenue. With the exception of providing a response to a request for a statement of reasons, there is **no obligation on Inland Revenue to form an opinion or create information** to answer a request.

If a requester seeks information by asking a question, there is a distinction between:

- questions which can be answered by providing information already known to and held by Inland Revenue (official information), and
- questions which require Inland Revenue to form an opinion or provide an explanation and so create new information to answer the request (not official information).

If a request is made for information that is **not** held by Inland Revenue, you need to consider:

- whether a valid request has in fact been made under section 12 of the OIA
- whether to transfer the request to another agency subject to the OIA or the Local Government Official Information and Meeting Act (LGOIMA), or
- whether to refuse the request under sections 18(e) or 18(g) of the OIA (because the requested document does not exist, or the information is not held).

However, there is nothing to prevent Inland Revenue from creating information in response to a request, if we choose to do so. Even if there is no information held by Inland Revenue that can be requested under the OIA, it may be administratively unreasonable for Inland Revenue to refuse to provide a response to the questions asked. If the person has any concerns about the response that they receive, then they can complain to the Ombudsman under the Ombudsmen Act 1975.

Information held by employees

Information which an officer, employee or member of Inland Revenue holds in their **official capacity** is deemed to be held by Inland Revenue.

Information held by Ministers of the Crown

The OIA applies to information held by a Minister of the Crown in their **official capacity** only. Official information does not include information which is held by a Minister:

- in their private capacity
- in their capacity as an MP (electorate information), or
- in their capacity as a member of a political party (caucus information).

However, such information may become official information if it is subsequently used for official Ministerial purposes.

Information held by independent contractors

Inland Revenue may contract private individuals, companies or other organisations to carry out particular work on their behalf.

Information which an independent contractor to Inland Revenue holds in that capacity is deemed to be held by Inland Revenue.

For examples of the types of information held by Inland Revenue, refer to Information Law at Inland Revenue

Tax confidentiality

When an OIA or Privacy Act request is made to Inland Revenue the first consideration is whether or not the information requested is sensitive revenue information and therefore confidential under the TAA. The requirements of the TAA will take precedence over the OIA and the PA.

Section 18(1) of the TAA requires all officers of Inland Revenue to keep confidential **sensitive revenue information**, unless the disclosure is permitted under sections 18D to 18J of the TAA. Also, they may not disclose **revenue information**, where disclosure of that information would adversely affect the integrity of the tax system or the maintenance of the law.

Is the information revenue information?

First determine whether the information is revenue information. **Revenue information** is defined in section 16C (2) of the TAA as any information acquired, obtained, accessed, received by, disclosed to, or **held** by the Commissioner—

- under or for the purposes of a revenue law; or
- under an information sharing agreement.

Revenue law is defined in section 16C(1), and includes:

- the Inland Revenue Acts;
- the Accident Compensation Act 2001, the Accident Insurance Act 1998, the Accident Rehabilitation and Compensation Insurance Act 1992, or the Accident Compensation Act 1982;
- the New Zealand Superannuation Act 1974; and
- any Act that imposes taxes or duties payable to the Crown.

An information-sharing agreement includes an approved information sharing agreement made under s 18E(2) of the TAA; an agreement made through consent under s 18E(3); agreements made by regulations under section 18F for public services purposes; and memoranda of understanding that IR has with other agencies to share information.

If the information is not held under or for the purpose of a revenue law, or under an information sharing agreement, consider the information under the PA or under the OIA. If the information is revenue information, next determine if it is sensitive revenue information.

Is the information sensitive revenue information?

Sensitive revenue information is defined in section 16C (3) of the TAA as revenue information that **relates to the affairs of a person or entity** and:

- identifies, or is reasonably capable of being used to identify, the person or entity, whether directly or indirectly; or

- might reasonably be regarded as private, commercially sensitive, or otherwise confidential; or

- the release of which could result in loss, harm, or prejudice to a person to whom or entity to which it relates.

"reasonably capable" of identifying a person or entity
The information does not necessarily of itself need to disclose a person/entity's identity but could enable someone to identify a person/entity. Whether information is reasonably capable of identifying a person/entity depends on the facts. For example, where the information disclosed could be combined with information that is publicly available to identify the person/entity then it may be reasonable capable of identifying a person or entity.

private, commercially sensitive, or otherwise confidential
Information "might reasonably be regarded" as private if it is reasonably foreseeable that information belonging to particular persons is of a type that the persons concerned would prefer is kept private. It is common practice to have confidentiality clauses in commercial contracts, particularly in a competitive industry. It is also reasonable to conclude that a company would want Inland Revenue investigating them kept private as it could damage their reputation.

commercially sensitive
What is commercially sensitive is usually measured in terms of the possible business harm or negative commercial effect through the disclosure of that information. The release of information of a commercial nature relating to a taxpayer should be approached with caution even if the information is anonymised. For example, in the course of a tax investigation we may come across information about a product that is being developed and kept secret pending an application for a patent.

otherwise confidential
This is a catch all provision - although it is difficult to see what information would be confidential on this basis that is not already private or commercially sensitive. However, it would cover any information reasonably regarded by the taxpayer/s to whom it relates as confidential. To determine this, as well as considering the nature of the information, it is necessary to consider the basis on which it was provided. So, for example, if the person provided the information on the condition that it was kept confidential, then the information may meet this requirement.

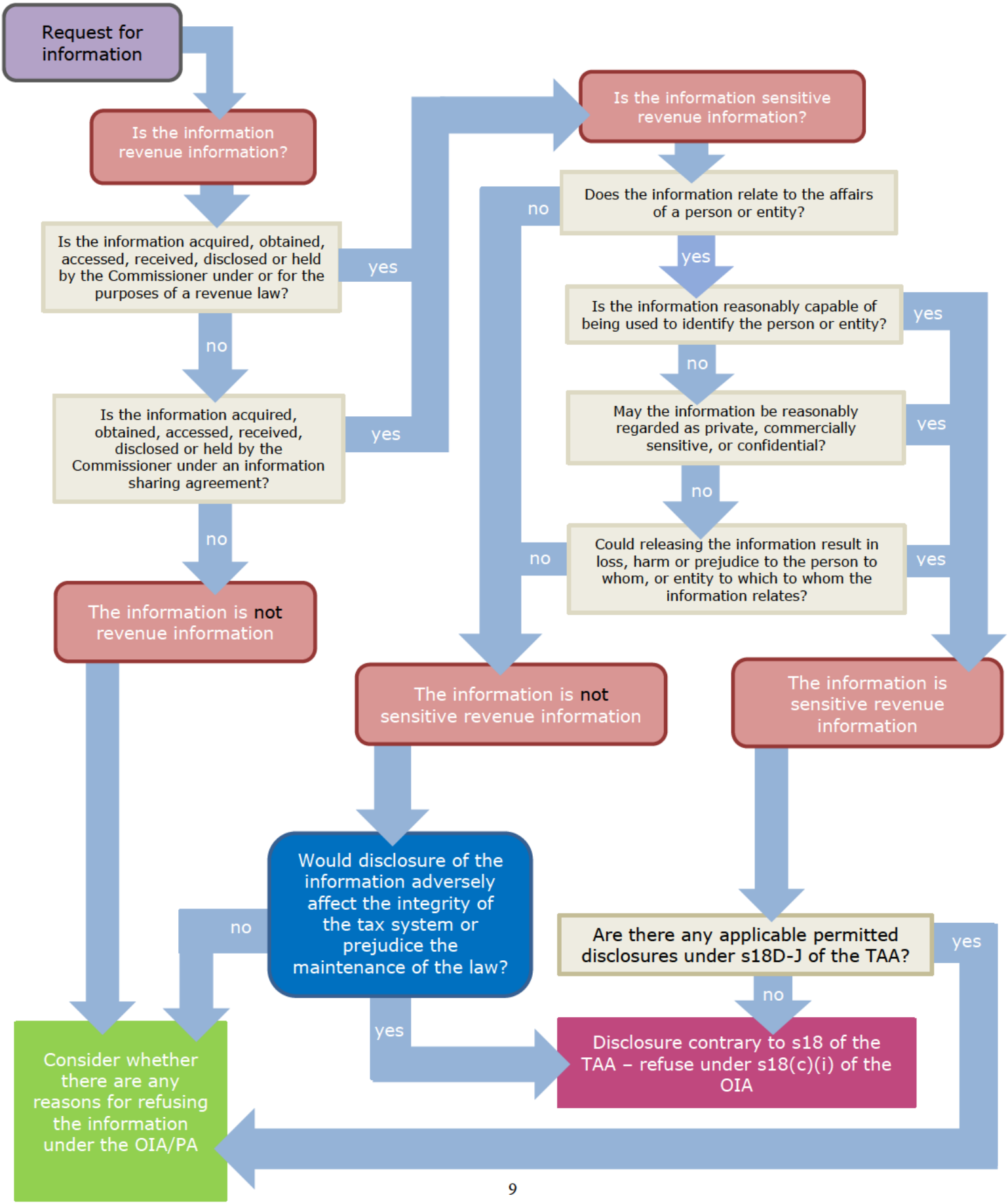
The release could result in loss, harm, or prejudice to a person to whom, or entity to which, it relates
As well as "commercially sensitive" information, this would also include all forms of potential damage or detriment to any person or entity to whom the information relates. It would include physical or non-physical harm, monetary and non-monetary loss, reputational harm, and any disadvantage resulting from being prejudiced.

Exclusion from sensitive revenue information
Aggregate data (suggests a grouping of things that are not necessarily numbers focused) and statistical data are explicitly excluded from being sensitive revenue information.

Aggregate or statistical data that may contain information about a person or entity is not sensitive revenue information.

If the information is **sensitive revenue information,** consider whether there is a permitted disclosure applicable under s18D – s18J of the TAA. If there is no applicable permitted disclosure refuse the request under s18(c)(i) of the OIA on the basis that disclosure of the information is contrary to the TAA.

Revenue information or sensitive revenue information? – flow chart



If the information is **not sensitive revenue information**, consider whether disclosure of that information would **adversely affect the integrity of the tax system or the maintenance of the law.** If it would not, the information should be considered under the PA or OIA as applicable.

Integrity of the tax system and maintenance of the Law

A request for revenue information should be refused if the disclosure of the information would adversely affect the integrity of the tax system or the maintenance of the law.

Before releasing revenue information, that is not sensitive revenue information, consider whether communicating the information "would adversely affect" taxpayer perceptions that tax liabilities are determined fairly and impartially, that all taxpayers must comply with the law, and that Inland Revenue keeps individuals' and entities' tax affairs confidential.

Consider the following questions when determining whether disclosure of the information would adversely affect the integrity of the tax system:

- What are the likely short and long-term effects on taxpayer compliance of releasing the information, and of not releasing the information?

- Could releasing the information assist Inland Revenue or taxpayers to make better decisions about how the current law applies, or assist in developing a better tax system?

- Could not releasing the information cause taxpayers to view Inland Revenue as unnecessarily secretive and unwilling to promote greater taxpayer participation in the tax system?

The following types of information are examples of information that if disclosed may adversely affect the integrity of the tax system:

- investigative techniques
- industry benchmarks
- audit strategy
- tolerance levels and thresholds
- new policy development

If releasing the information is likely to have negative effects on compliance that outweigh any benefits to tax integrity from releasing it, then a request for the information should be refused under s18(c)(i) of the OIA on the basis that disclosure of the information is contrary to the TAA.

Example
Information about generic audit or investigative techniques would be revenue information which is not sensitive revenue information because it is revenue information that applies generally and does not relate to a particular person. However, releasing this information is likely to have a material negative impact on taxpayer compliance because some taxpayers may attempt to use it to avoid their tax obligations. This negative impact is likely to outweigh any benefits to the integrity of the tax system from releasing this information (from, for example, increased transparency). Therefore, the information should not be released.

Another reason for not disclosing revenue information that is not sensitive revenue law is where the maintenance of the law would be prejudiced. This includes tax laws and laws administered or maintained by other agencies.

The OIA and PA both have a ground for refusing information on the basis of "maintenance of the law". The Privacy Act allows agencies to collect, withhold, use or disclose personal information where it is necessary for the 'maintenance of the law'. Under the OIA and PA maintenance of the law relates to law enforcement action by a public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences.

These reasons only require the maintenance of the law to be "prejudiced". This does not require the maintenance of the law to be negated or nullified. It would be enough if release could have a compromising or detrimental effect.

Example would be where the Police have informed Inland Revenue that they are investigating a possible scam in a particular part of New Zealand. They have asked if Inland Revenue has any specialised investigative techniques that Inland Revenue uses in countering organised crime. The media has subsequently asked if Inland Revenue has been approached by the Police regarding any investigation into the suspected scam, and if so, in which location in NZ. This information would not be able to be released under the OIA if disclosure would prejudice the maintenance of the law by compromising the Police investigation.

Permitted Disclosures of sensitive revenue information

Sensitive revenue information can only be disclosed if doing so is a "permitted disclosure" under sections 18D-J of the TAA.

Carrying into effect - s18D(1)
Sensitive revenue information can be disclosed for the purpose of carrying into effect a revenue law, or for the purpose of performing or supporting a function lawfully conferred on the Commissioner under a revenue law.

Example
A customer has income tax arrears. You have issued a deduction notice, instructing the taxpayer's bank to deduct a sum of money. In this way, you have disclosed to the bank that the customer has tax arrears. This disclosure, however, is necessary for the purposes of carrying into effect the TAA.

Carrying out or supporting a function of the Commissioner – s18D(2)
Sensitive revenue information can be disclosed under this section by a senior member of Inland Revenue with appropriate delegation, who has considered competing factors to reach a judgement that a disclosure is reasonable in the particular circumstances (guidance on the application of s 18D(2) can be found in Standard Practice Statement 11/07).

The first step is to assess if disclosure would be made in carrying out or supporting a function of the Commissioner. The functions of the Commissioner include:

- administering the tax system
- implementing the tax system, and
- improving, researching or reforming the tax system.

The second part of the test is to determine whether disclosure would be reasonable, after weighing and balancing the following five factors:

1. the Commissioner's obligation at all times to use best endeavors to protect the integrity of the tax system, and
2. the importance of promoting compliance by taxpayers, especially voluntary compliance, and
3. any personal or commercial impact of the communication or in any other way, and
4. the resources available to the Commissioner, and
5. the public availability of the information.

Disclosures to persons and their representatives – s18G
Sensitive revenue information can be disclosed to the person (or their agent) in relation to whom the information is held. Clause 15 of schedule 7 of the TAA sets out caveats on provision of personal information. The Commissioner must consider whether –

- the information is readily available; and
- if it is "reasonable and practical" to provide the information.

If the information is not "readily retrievable" –

- if the request is by or on behalf of an entity the request may be refused under s.18(c)(i) of the OIA on the basis that the information is sensitive revenue information and there is no permitted disclosure
- if the request is by or on behalf of a natural person the request may be refused under s.29(1)(i) of the PA on the basis that the information is sensitive revenue information and there is no permitted disclosure

If we consider that the disclosure of the information would adversely affect the integrity of the tax system. Although the information may be personal information, there would not be a permitted disclosure as it would not be "reasonable and practical" for the Commissioner to disclose the information.

Other permitted disclosures
Other permitted disclosures that will not usually be relevant in the context of an OIA/PA request.

Seek any advice as required, from subject matters experts, LTS, Corporate Legal, or Inland Revenue's Privacy Officer.

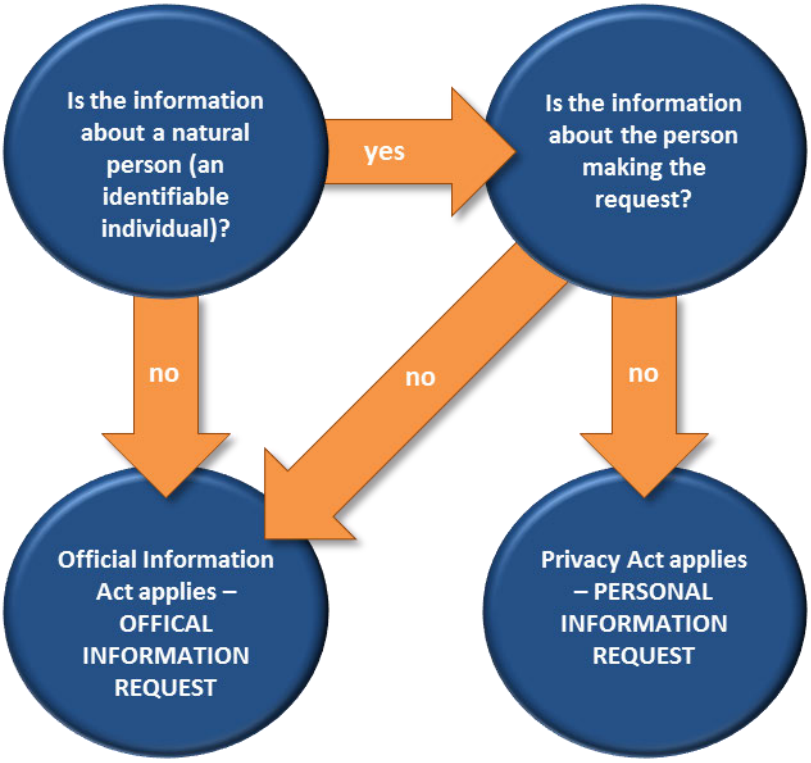
Eligibility to request official information

OIA and Privacy interface

If you have concluded that you are permitted to disclose the information requested under the TAA, then you may consider the Official Information Act 1982 (OIA) and the Privacy Act 1993 (PA). The OIA and PA are two pieces of legislation that govern most information requests. You first need to work out which Act applies:

- When an individual asks for information about themselves, the PA applies; this includes requests from a person's authorised agent.
- When the request is from someone else, the OIA applies.

The following flow chart can be used to determine whether the request should be considered under the OIA or PA.



Who can make an OIA request?

Any person is entitled to make a request under the OIA who is:

- a New Zealand citizen
- a permanent resident of New Zealand

- a person who is in New Zealand
- a body corporate which is incorporated in New Zealand
- a body corporate which is incorporated outside New Zealand but which has a place of business in New Zealand, or
- a duly appointed agent acting on behalf of any of the above.

Who can make an PA request?

Any person is entitled to make a request under the PA for information about themselves. Such request can be made by a duly appointed agent. Inland Revenue is entitled to satisfy itself as to the requester's eligibility to make a request under the OIA or PA.

If a request is made by email or over the internet, system verification may be required to confirm eligibility. If you are still uncertain as to whether the request is valid or not, you are entitled to ask reasonable questions to check whether the person is eligible to make a request. If you do wish to query eligibility, please do so promptly so as to not unnecessarily delay the processing of a valid request.

What if a requester is not eligible?

Even if a person is not eligible to make a request for official information under the OIA (for example a person who is overseas and not a New Zealand citizen or resident), they can still ask an agency for the information they are seeking.

Although Inland Revenue isn't required to respond in accordance with the requirements of the OIA, we should still deal with the request for information in an administratively reasonable manner. If the person has any concerns about the response that they receive, then they can complain to the Ombudsman under the Ombudsmen Act 1975.

The form of an official request

What does an OIA request look like?

There is no set way in which a request must be made. An OIA request is made in any case when an eligible person asks Inland Revenue for access to specified official information. In particular:

- a request can be made in any form and communicated by any means, including orally
- the requester does not need to mention that it is an OIA or Privacy Act request, and
- the request can be made to any person in Inland Revenue.

If a request is made orally, we may ask the requestor to put it in writing if that's "reasonably *necessary"* to clarify the request. If the requester declines or is unable to do

so, then we should record our understanding of the request and provide a copy of that record to the requester.

The working-day count will start the day after the requester confirms or clarifies Inland Revenue's understanding of the request is correct.

"Due particularity": a requester's obligation

To be a valid request, the information sought must be *'specified with due particularity'*. This means that Inland Revenue must be reasonably able to identify what information is being requested.

When you receive a request:

- consider the request carefully
- identify the specific information that has been requested
- consider the scope of the request, and
- the relevant time period the requester has identified.

If there is any doubt about the scope of the information requested, you will need to clarify this with the requester as soon as possible.

Is a formal OIA/PA response necessary?

For Inland Revenue to meets its obligations under the OIA and PA, every information request must be accurately recorded and counted. Inland Revenue regularly receives requests for information through a variety of channels: phone, email, letters etc. At times, it's not easy to decide if the request is an official request that requires consideration and a formal response under the OIA or PA. To help you decide if a formal response is needed, ask yourself the following questions:

To respond to the request, do you need:

- manager approval/oversight
- consultation with others, or
- significant staff time?

Also, do you need to withhold (redact) some or all of the information requested?

If any one of the above applies, then the request must be recorded and counted to avoid the risk of Inland Revenue not complying with the OIA/PA's requirements.

Examples of Official Information requests

- A Member of Parliament requests all information about specific Inland Revenue spending.
- A journalist requests statistical data on a particular tax type.
- A taxpayer requests information about a specified tax type and details on how many outstanding returns there are for a stated city or region.

- The media requests information about IR's announcements /releases.
- A researcher has requested all policies relating to GST rates.

Examples of Privacy Act Requests

- A customer requests their own records that are with Investigations and Advice.
- A customer requests a copy of their administrative review and statement of financial position.
- A customer requests all information from the start of their student-loan account.
- A staff member requests information from their personal file.
- A customer requests an audio recording of a phone-call they had with Inland Revenue on a specified date/time.

Large requests

The fact that a request is for a large amount of information does not mean that the request lacks due particularity. The term "fishing expedition" is not recognised in the OIA as a reason to refuse a request. If the information requested is duly particular, the request cannot be refused simply on the basis that it's so large as to be considered a fishing expedition.

If there are genuine administrative concerns with processing the request or making the information available, the reasons for refusal under section 18 of the OIA may need to be considered, along with other mechanisms for managing broad requests.

Amended or clarified requests

Section 15(1AA) and (1AB) of the OIA deal with *"amended or clarified requests"*.

If a request is amended or clarified after it is made, it can be treated as a new request which replaces the original one. This voids Inland Revenue's obligation to respond to the original request, and starts again the statutory time limit for responding to the new request.

However, this will not apply where the amendment or clarification was sought by Inland Revenue more than seven working days after receiving the original request.

The primary intention of these provisions is to identify and clarify problematic requests early on.

Although this may sound straightforward, the effect of this section will depend on various factors, including:

- whether the amendment or clarification was sought by Inland Revenue or made on the requester's own initiative
- whether the amendment or clarification is actually received after it is sought by the agency and, if so, when, and

- whether the "new" request is intended to amend or clarify the terms of the original one, or to be separate and additional to it.

The following scenarios may arise:

Requester amends or clarifies the request on their own initiative.	The new request replaces the original one, and the 20 working-day **time limit for responding starts the day after the new request is received**. IR has no further obligation to respond to the original request. **NB**. It must be clear that the new request is intended to replace the original request by amending or clarifying its terms. This will not apply where the new request is clearly intended to be separate and additional to the original one.
IR seeks amendment or clarification **within 7 working days** and **the** amendment or clarification is **received within 20 working days**	The new request replaces the original one, and the 20 working-day time limit for responding starts the day after the new request is received. IR has no further obligation to respond to the original request.
IR seeks amendment or clarification within **7 working days** and amendment or clarification is **not received within 20 working days**	The original request still stands, and to ensure that it complies with its obligations under the OIA, IR must, **within the original** 20 working days, either extend the time limit for responding (to enable consultation with the requester) or convey its decision on the request. IR will need to consider whether the request can be granted as it stands, or whether extending or charging would enable it to be granted or, as a last resort, whether the request must be refused under one (or more) of the applicable refusal grounds.
IR seeks amendment or clarification **outside 7 working days** and amendment or clarification is received **within 20 working days**	Provided that what is received is in fact an amended or clarified version of the original request, then the maximum 20 working-day time limit for responding to that request still counts **from the day after the original request was received.** Within that time, IR must either extend the time limit for responding, or convey its decision on the request. However, if a completely different request is received (as opposed to an amended or clarified version of the original request), that will be **a new request** and the 20 working day time limit for responding will start the day after that request was received. **Note**. It must be clear that the new request is intended to replace the original request. If there is any doubt about this, it may be wise to check with the requester.

IR seeks amendment or clarification **outside 7 working days** and amendment or clarification is **not received within 20 working days**	The original request still stands, and to ensure that it complies with its obligations under the OIA, IR must, within the original 20 working days, either extend the time limit for responding (to enable consultation with the requester), or convey its decision on the request. IR will need to consider whether the request can be granted as it stands, or whether extending or charging would enable it to be granted, or, as a last resort, whether the request must be refused under one (or more) of the applicable refusal grounds.

A duty to assist requesters

Inland Revenue has a duty to give reasonable assistance to a person who:

- wishes to make a request in accordance with section 12 of the OIA or the PA
- in making such a request, has not done so in accordance with the requirements of the OIA or PA, or
- has not made the request to the appropriate agency.

If Inland Revenue cannot reasonably identify what information is being requested, then there is a duty on Inland Revenue to give reasonable assistance to the requester to reformulate the request in order to determine exactly what information is being requested.

Reasonable assistance is more than telling the requester that the request is not specific. Having regard to the purposes of the OIA and the principle of availability, all reasonable steps should be taken to provide assistance. The aim of the assistance should be to enable the requester to clarify the request so that it is specific enough for Inland Revenue to identify the information sought.

The key is to communicate with the requester. If a request isn't clear, contact the requester and explain what you need to help them.

What is reasonable assistance?

Reasonable assistance may include things like:

- providing an outline of the different kinds of information which might meet the terms of the request
- helping the requester understand the general nature and extent of information held by Inland Revenue (at a high level)
- providing a general response to the request, setting out options for further information which could be provided on request, and
- giving the requester a reasonable opportunity to consult with a contact person.

Processing requirements

How should I document OIA requests?

The knowledge base currently includes processing instructions for various business groups.

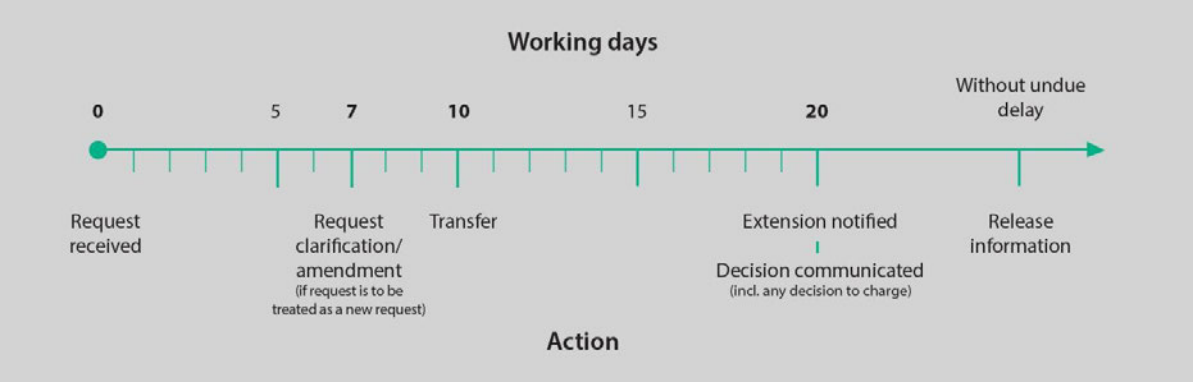
The following key points need to be included in system updates and/or reports/ sign off check sheets to ensure all relevant information is captured for reporting and reviewing purposes.

Record:

- the date the request was received
- the request identifier (reference number, e.g. 19/OIA0012)
- the information requested
- any contact/clarification with customer
- the outcome of the contact
- any transfers or extensions of time needed
- a copy of what was released
- what was withheld and why
- the factors considered in making the decision, e.g. internal advice, emails
- the time taken to complete the request
- evidence of consultation with other agencies or any internal consultation
- reference legislation and DLN numbers of the information sent out
- the revenue delegation level, name and position title of who had the authority to approve the release or withholding of the information
- Government and Executive Services sign off – if applicable.

All requests for information should be lodged with Government and Executive Services by sending a copy of the request to oia@ird.govt.nz.

Key timeframes



Inland Revenue's legal timeframe requirements for responding to requests for official information are to:

- **make a decision and communicate it** to the requester *"as soon as reasonably practicable"* and no later than **20** working days after the request is received, and
- **make available** any official information it has decided to release without *'undue delay'*.

Where necessary in a particular case, additional timeframe requirements are to:

- **request clarification** of a request within **seven** working days, if the amended request is to be treated as a new request
- transfer a request to another agency promptly, and no later than **10** working days, after the request is received, and
- **extend** the maximum time limits to make a decision or transfer a request, within **20** working days after the day on which the request was received.

How to count time

A tool to automatically calculate response times is available on the Ombudsman's website at www.ombudsman.parliament.nz. You find information about OIA requests and access the Ombudsman's time calculator via the Stakeholder Relations intranet page.

When counting working days, day one is the first working day after the day on which Inland Revenue receives the request.

"Working day" means any day of the week other than Saturday and Sunday and excludes national public holidays: Waitangi Day, Good Friday, Easter Monday, Anzac Day, Queen's Birthday, Labour Day, and from 25 December to 15 January inclusive.

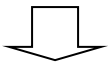
A regional anniversary is a working day.

A working day is not limited to 9am to 5pm. Therefore, if a request is received by email or other electronic means outside business hours, it will still be counted as being received on that day, and the count will start on the next working day.

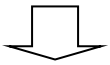
Examples of how to count time

Example 1

Inland Revenue receives an information request by email at 9pm on 6 October 2019 (Sunday).

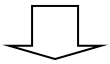


The working day after which the request is received = 7 October 2019 (the time and that it is received is irrelevant).



Public holidays that don't count in the 20-working-day timeframe:

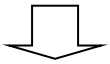
- Labour Day = 28 October 2016



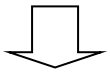
The 20-working-day maximum time limit is **4 November 2016**.

Example 2

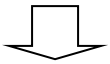
Inland Revenue receives an information request at 3pm on 21 December 2019 (Saturday).



The working day after which the request is received = 23 December 2019 (Monday).



The days between 25 December to 15 January of every year are not "working days".



The 20-working-day maximum time limit is **10 February 2017**.

There is a calculator on the Ombudsman's web-site which can help you work out the maximum timeframe for when a response is required, at www.ombudsman.parliament.nz.

Timeframe for making and communicating a decision

Inland Revenue must make a decision and communicate it to the requester *"as soon as reasonably practicable"* and no later than 20 working days after the day on which the request is received.

The decision must state whether the request will be granted, and if so in what manner and for what charge (if any).

Inland Revenue's primary legal obligation is to notify the requester of the decision on the request *"as soon as reasonably practicable"*. The reference to 20 working days is not the de facto goal but the **absolute maximum** (unless it is extended appropriately).

Timeframe for making information available

If a decision is made to release information, then we must not unduly delay in making it available. In some cases, Inland Revenue may be justified in providing the information to the requester at a later date, after the decision is made and communicated within the timeframe.

Note. The distinction between the time requirements for making and communicating a decision on a request, and for making information available, can be important, especially when responding to large requests. Ideally, where a request is granted, the decision and the information will be sent to the requester together. If the information is ready to be released at that stage, not to send it would amount to *'undue delay'*. However, that may not always be possible and sometimes we may need extra time to prepare the information for release.

For instance, we may know that we intend to grant a request subject to some redactions but the process of preparing the material for release will take a bit longer. We can advise the requester of our decision on the request as soon as reasonably practicable and within the maximum 20 working-day time limit, and give an indication of when we will be in a position to release the information requested. Our decision must still comply with the OIA, but so long as there is no 'undue delay' in making the information available there will be no breach of the timeframe requirements in the OIA.

Transferring a request

The OIA and PA require requests to be transferred between agencies in certain circumstances.

Transfers are not common with requests for entity-specific tax information.

Transfers can be made between any agencies subject to the OIA or Local Government Official Information and Meetings Act 1987 (LGOIMA), including Ministers, central government agencies and local government agencies.

Refer to the template letters for transferring a request to another agency, and advising the requester of the transfer.

The obligation to transfer

Inland Revenue **must** transfer a request to another agency if some or all of the information requested:

- is not held by Inland Revenue, but is believed by the person dealing with the request to be held by another agency, or
- is believed by the person dealing with the request to be more closely connected with the functions of another agency.

The obligation to transfer is not discretionary, but a mandatory requirement in circumstances either of the above two criteria are fulfilled.

Example

A parent (the child's principal caregiver) asks Inland Revenue for a copy of all information relating to their Working for Families (WFF) tax credit payments for 2015. Although Inland Revenue may have some information, the information is more closely connected with MSD as MSD has been paying the WFF tax credit.

In the absence of these circumstances, a request cannot be transferred. Therefore, as receiver of the request, Inland Revenue must make the decision on it. However, this does not prevent Inland Revenue from consulting other interested parties before making the decision.

The OIA does not support a blanket policy of transferring all requests from a particular source (for example, media requests), or all requests about a particular subject. It is the specific **information requested** that must be held by the other agency or more closely connected with its functions, and this must be assessed on a case by case basis.

Deciding if information is "more closely connected" with another agency

The following factors can be considered in deciding whether information is more closely connected with another agency's functions:

- The author of the information—if another agency wrote it, maybe they should decide on the request.
- The nature and content of the information—which agency does the information relate to; which agency will be called to account for the information?
- The overall process that the information forms part of—which agency has responsibility for that process?

Partial transfers

Where the above circumstances only apply to part of the information requested, only the relevant part of the request should be transferred, rather than the request in its entirety. The transfer should make it clear what parts of the request are being retained by Inland Revenue and what parts are being transferred.

Example:

An official information request has been received from a customer who wants copies of information used to calculate and determine the level of benefit they are currently receiving and a copy of their Working for Families (WFF) tax credit calculation for the current year. The customer has elected that Inland Revenue pays the WFF tax credit. As the benefit information is not held by IR, this part of the request must be transferred to MSD within 10 working days and the customer advised of the partial transfer.

Timeframe for transferring a request

Any decision to transfer a request to another agency for response must be made promptly and no later than **10 working days** after Inland Revenue received the request. (Unless a

valid extension of that time limit is made within 20 working days of the original request.) The requester must be informed that the request has been transferred.

When the other agency receives the transferred request, it is effectively a new request made to that agency under the OIA. The working day count, in terms of the maximum time limit for making and communicating a decision, begins again when they receive the request.

Note: The OIA is clear—the need to transfer a request is something that every agency should identify and action as early as possible. An extension to the maximum time limit of 10 working days for transfer may be made, for example where the relevant agencies are consulting about the proposed transfer. However, if a request is transferred outside the maximum (or extended) time limit, this could potentially be the subject of complaint to the Ombudsman under the Ombudsman's Act (OA) and a potential finding that the agency had acted *'contrary to law'*.

Having said that, a delay will not invalidate the transfer. Even if a transfer is made out of time, it will still have the effect of shifting the responsibility for reaching a decision on the request to the most appropriate agency. That is, after all, what the transfer provision is about—ensuring that the agency that holds the information, or that is best placed to know whether there are valid concerns about disclosure, makes the decision on the request.

If Inland Revenue identifies the need to transfer all or part of a request outside the 10 working days (or extended time period), we should consider contacting the requester to explain the reason for the delay and the need for the transfer. Requesters will appreciate being kept informed, and may be more understanding if the agency ends up in breach of the timeframe requirements.

Consulting about the proposed transfer

It may be a good idea to consult the requester and/or the other agency before transferring a request.

The requester can clarify why they made the request to Inland Revenue, and what information they hoped to obtain. They may be interested in knowing what Inland Revenue holds in connection with its functions, and not what the "lead agency" on a particular issue holds.

Consulting with the other agency will enable you to make appropriate arrangements for the transfer. It is helpful to ask the other agency:

- Have they already received the same request?
- Are they the right agency to receive the transfer?
- Who within the other agency should the transfer be addressed to?

Consulting will also minimise the risk of "bounce-backs", where the other agency disagrees that the information is more closely connected with its functions, and returns the request to Inland Revenue.

What if the other agency already has the same request?

Sometimes, your consultation about a proposed transfer will reveal that the other agency is already dealing with exactly the same request. In this instance, it's probably pointless to make the transfer. You could try discussing the situation with the requester. They will likely want an assurance that Inland Revenue doesn't hold any additional relevant information that the other agency won't have, and they may end up withdrawing their request if such an assurance can be given. Alternatively, you could respond to the requester along the following lines:

In our view, it would have been necessary under section 14 of the OIA to transfer your request to [agency] because the information you requested is [held by that agency / more closely connected with its functions]. However, we are aware that you have already made your request to [agency], and therefore we have not transferred it. [We do not hold any additional relevant information that is not already held by [agency] / We have provided copies of all additional relevant information that we hold to [agency] for consideration in responding to your request] You have the right to complain to the Ombudsman about this decision. Relevant information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Transfers between Ministers and agencies

In determining whether information is more closely connected with a Minister's or an agency's functions, it can be helpful to consider the role of the Minister.

Ministers:

- take significant decisions and determine government policy collectively, through the Cabinet decision-making process
- exercise statutory functions and powers under legislation within their portfolios, within the collective Cabinet decision-making context
- determine both the policy direction and the priorities for their departments, and
- have a political role in maintaining government stability, which requires maintaining close working relationships with all other parties as issues arise.

If the information relates to executive government decision making functions, and release could prejudice Cabinet's or the Minister's ability to perform those functions, then transfer to the Minister may be justified. If the information relates more closely to operations and policy implementation, then the agency should probably be responsible for deciding on the request.

Even if a transfer is not warranted, there is nothing to prevent an agency consulting its Minister (see the "Consulting Ministers" section).

If consultation leads to disagreement about the appropriate response to a request, this is not, in itself, a reason to transfer. The person dealing with the request must have a genuine belief that the information is more closely connected with the Minister's functions before transfer can legitimately occur. If disagreements arise, these should be handled at a senior level of the agency.

In any case, it is important that the transfer of the request does not have the effect of narrowing its scope or excluding relevant information. The agency that received the

request should identify the relevant information first and, if necessary, transfer that information along with the request.

Extensions of time

Inland Revenue may extend the maximum time limits for **making a decision and communicating it** to the requester and also for **transferring a request** – but only if certain criteria are met. These are:

- there must be a valid reason for the extension, either:
  - the request is for a large quantity of information or necessitates a search through a large quantity of information, and meeting the original time limit would unreasonably interfere with the operations of Inland Revenue; or
  - consultations necessary to make a decision on the request are such that a proper response to the request cannot reasonably be made within the original time limit.
- the extension must be for *"a reasonable period of time having regard to the circumstances"*; and
- the decision to extend the maximum time limit must be communicated to the requester within 20 working days after the day on which the request was first received by Inland Revenue.

When making an extension, Inland Revenue must advise the requester:

- that it has decided to extend the time limit
- the specific period of the extension
- the reasons for the extension
- the section of the OIA or PA the request is being extended under, and
- that the requester has a right to complain to the Ombudsman or the Privacy Commissioner about the extension decision.

To keep things simple when giving the period of the extension, it may be helpful to specify a date rather than the number of working days or weeks when the response can be expected.

Nothing in the OIA prevents multiple extensions being made, providing any extensions are made **within** the original 20 working-day time period after receiving the request. For example, if Inland Revenue notifies the requester of a one-week extension, and then later realises that a two-week extension is actually necessary, a second extension may be notified as long as the original 20 working-day time period has not yet passed.

To avoid confusion, it may be better to make one extension, for a reasonable but realistic period of time, and indicate that Inland Revenue will respond to the request sooner if possible.

Failure to meet the maximum time limits

If it looks like it will not be possible to meet either the original or an extended maximum time limit, Inland Revenue should consider contacting the requester to let them know the current state of play and reasons for the delay. Requesters will appreciate being kept informed, and may be more understanding if Inland Revenue ends up in breach of the timeframe requirements.

Another option is a staged reply. If most of the decision on a request is straightforward and ready to go, there is often no need to hold that up in order to deal with a few remaining issues.

However, failure to comply with a time limit may be the subject of a complaint to the Ombudsman.

Requests for urgency

A requester may ask that a request is treated as urgent, and if so must give the reasons for seeking the information urgently. Inland Revenue should consider any request for urgency, and assess whether it would be reasonable to give the request priority.

Notwithstanding a request for urgency, Inland Revenue's legal obligations remain the same – in other words, to:

- make and communicate the decision on the request as soon as reasonably practicable and no later than 20 working days after the day on which the request was received, and
- release any official information without undue delay.

A genuine and legitimate need for urgency may affect when it is *'reasonably practicable'* to make a decision on the request, and what would constitute *'undue delay'* in releasing the information.

In responding to a request for urgency, Inland Revenue should:

- assess the requester's reasons for seeking urgency (do they merit the request being accorded priority over other work, including other information requests?)
- decide whether to accord urgency to the request, and
- advise the requester of this decision, and (if applicable) provide an indicative timeframe for response.

Inland Revenue can consider discussing an urgent request with the requester. This may enable:

- Inland Revenue to clarify the competing priorities that would need to be side-lined in order to accord urgency to the request
- requesters to clarify the reasons for urgency, in light of these competing priorities, and
- requesters to clarify the intended scope of their request, or to prioritise particular information, allowing decisions on certain information to be made sooner rather than later.

The OIA makes it clear that charges may be imposed to cover the costs incurred pursuant to a request to make information available urgently.

A requester who is dissatisfied with Inland Revenue's response to an urgent request may complain to the Ombudsman that Inland Revenue has failed to make and communicate its decision on the request *"as soon as reasonably practicable"*, or to release the information without *"undue delay"*.

Urgent requests are often made in order to enable the requester to participate in a consultation or decision-making process on an informed basis. If you can see that this is a valid concern in the context of the particular request at issue, you could consider extending the deadline for participation. This may enable the information to be released and used by the requester, without imposing an unreasonable burden on Inland Revenue to comply with an urgent request.

Consultation

Inland Revenue may consult before making a decision on an official information request. When consulting externally, staff should bear in mind their confidentiality obligations under the TAA.

Consultations may be with:

- the requester
- relevant business areas within IR, such as Government and Executive Services, LTS, the Internal Communications Team and other Inland Revenue specialists.
- external third parties, e.g. those who originally provided the requested information to Inland Revenue, or whom the information is about, and
- any other agency with an interest in the information, including Ministers.

Any consultations should be necessary for Inland Revenue to make a proper decision on the request. If there are unnecessary consultations and sign-offs taking place, this could give rise to a complaint that Inland Revenue has failed to make and communicate its decision on a request *'as soon as reasonably practicable'*.

When consultations are being undertaken, Inland Revenue should consider:

- whether the maximum time limit for responding to the request needs to be extended
- whether all or part of the request must be transferred to another agency, on the basis that its functions are more closely connected with the requested information
- whether a decision can be made in respect of some of the information requested while consultations on the remaining information are under way, and
- speaking to the requester to explain the need to consult with others.

Although the requester is not obliged to do so, they may be able to clarify why the information is being requested. This often helps to expedite or inform the consultation process. Equally, the requester may be able to narrow or limit the request so that any consultation is no longer necessary.

Consulting requesters

Consulting requesters can be very useful when considering a request. The reasons for consultation can include:

- confirming the exact nature of the information requested
- explaining any difficulties Inland Revenue is having in processing the request (for example when there is a large amount of information at issue), and allowing the requester to consider amending or refining the scope of the request, and

- informing the requester if there are likely to be any delays in processing their request.

Often there may be a perception that agencies are unwilling to provide information or are deliberately seeking to delay or to hide information due to a lack of understanding about the process. If there is going to be a delay for any reason, it is important to let a requester know the reasons for this.

Inland Revenue can consult with requesters for any reason. However, the OIA specifically requires agencies to consider consulting them before refusing a request on the basis that the information does not exist or cannot be found, despite reasonable efforts to locate it, or the information cannot be made available without substantial collation or research.

Consultation with a requester may result in an amended or clarified request. The implications of this for our statutory obligations are discussed above, under "Amended or Clarified Requests".

Consulting third parties - Commercial sensitivity considerations s18

There is no requirement under the OIA for agencies to consult external third parties before making a decision on a request. However, we should consider whether it is necessary to do so if:

- the information is about the third party
- the information was supplied by the third party, and/or
- release could adversely affect the third party.

This will often be relevant if we are proposing to release information that may raise privacy, confidentiality or commercial concerns.

Notwithstanding the outcome of any consultation, the decision on the request for information remains with Inland Revenue to take. We should consider what the third party has to say, and reach an own independent view on the applicability of any withholding grounds, and the public interest in release.

The OIA provides protection for agencies that **release information in good faith** in response to a request. However, a complaint may potentially be made to the Ombudsman under the Ombudsmen Act that an agency has acted unreasonably in either omitting to consult an external third party, or in how they went about that consultation, or in deciding to release the information notwithstanding consultation.

What information should I include when consulting external third parties?

An efficient and effective consultation should include the following matters:

- Sufficient relevant background information about the request.
- The identity of the requester (unless there is specific good reason not to provide this). Good administrative practice is to advise the requester of the intended consultation first to check that there are no genuine concerns about disclosure of the requester's identity. If the requester wishes to remain anonymous, Inland Revenue should consider whether there is a reasonable basis for non-disclosure, given that the identity of the requester may often be a relevant factor for a third party in identifying any concerns with release of the information requested.
- A copy of the information at issue if the third party does not already hold it, or a brief description of the information Inland Revenue holds which is captured by the request and on which we are seeking the third party's comments.
- Advice about the agency's obligations under the OIA for responding to the request for this information, including that:
    - the agency must follow the principle of availability set out in the OIA
    - it is for the agency to assess whether there is 'good reason' for withholding information
    - third parties can expect their concerns to be taken into account, but they cannot veto release, and
    - lack of consent is not, in itself, a reason for refusal.
- A request for confirmation as to whether the third party has any concerns with release and if so, a detailed explanation of these and the basis for them.
- A date for response to enable the agency to make a timely decision on the request.

Consulting Ministers

Responsible Ministers often have a legitimate interest in OIA requests received by their agencies. Agencies are permitted to consult Ministers about the decision they propose to make on an official information request. However, Inland Revenue officers have tax confidentiality obligations under the TAA (whereas Ministers do not). This means that we should only be providing Ministers with information where an exception to confidentiality applies.

The most relevant exception may often be the one set out in section 18D(2) of the TAA, that disclosure supports a "function of the Commissioner" (note that this must be a tax-related duty and does not include the duty to respond to official information requests) and is "reasonable" regarding the factors set out in section 18D(2).

In practice, this means we should only be notifying the Minister of requests where we consider there is a real need to, such as where we are seeking the Minister's opinion on the appropriate approach to the request (bearing in mind that this is still ultimately our decision), or where we have a contentious or topical request that may receive some publicity.

Where consultation with the Minister(s) is considered appropriate, one way to do this is to provide advance notice to the Minister of the request, the information at issue, and the

decision Inland Revenue plans to take. Under the "no surprises" principle, request should be sent to the Minister's office **five** working days prior to the statutory due date.

Consultation arrangements should be configured so that Inland Revenue can meet our requirement to make and communicate the decision on a request within the maximum 20 working days. Accordingly, Inland Revenue should endeavour to provide advance notice to the Minister's office well before the maximum 20 working days expire (for instance, around the 10 to 15 working-day mark).

Government and Executive Services (GES) is responsible for coordinating communication between Inland Revenue and the Minister's offices. GES is the first point of contact for advice and guidance on contacting a Minister.

Making a decision

Considering whether to grant the request

When making a decision on an OIA request, Inland Revenue must decide:

- whether the request will be granted, and if so
- in what manner, and
- for what charge (if any).

Inland Revenue must then communicate that decision to the requester as soon as reasonably practicable and no later than 20 working days after the day on which the request was received (unless the maximum time limit is extended).

Information that comes to be held after a request is received

IR may receive or generate additional relevant information after a request is received but before a decision is conveyed. Technically, a requester is only entitled to request information 'held' (i.e. in existence) at the time of their request. However, there is nothing to prevent Inland Revenue from considering the additional relevant information in conveying our decision on the request. It may be reasonable to do so if there is no practical reason not to, and it is clear the requester would want to obtain the additional relevant information. At the least, Inland Revenue should make it clear to a requester if additional relevant information has come into existence which has not been captured by the scope of the request, so they may request it if they wish.

Which part of the OIA applies?

Different rules apply to different type of requests. It is important to be aware of which rules apply, in order to ensure that the right decision is made.

Part 2 OIA: General requests for access to official information that is not about the requester.

Part 3 OIA: Requests under section 22 for access to an agency's policies, principles, rules or guidelines for making decisions or recommendations in respect of any person.

Part 3 OIA: Requests under section 23 for a written statement of reasons why a decision or recommendation was made about the requester.

Part 4 OIA: Requests by a corporate entity for information about itself.

Deciding how to release information

If the decision is to grant the request, Inland Revenue must also decide how the information will be released.

There are a number of different ways to make information available. Inland Revenue can:

- give the requester a reasonable opportunity to inspect the information (e.g. when a staff member reviews a piece of information on their personnel file)
- release a hard copy of the information
- release the information in electronic form or by electronic means
- arrange for the requester to hear or view the information
- provide a written transcript of the information
- provide partial disclosure of the information, e.g.:
    - release a document with some information deleted (redacted)
    - release a summary of the information
    - release an excerpt, or particular passage, from a document, or
- provide the requester with an oral briefing.

However, Inland Revenue must release the information in the way preferred by the requester, unless to do so would:

- impair efficient administration
- be contrary to any legal duty we have in respect of the information
- prejudice the interests protected by section 6, 7 or 9 of the OIA (and in the case of the interests protected by section 9, there is no countervailing public interest), or
- prejudice the interests protected by section 27 or section 28 or section 29 of the PA and (in the case of the interests protected by section 28) countervailing public interest.

If information is not provided in the way preferred by the requester, Inland Revenue must explain the reason for not providing the information in that way and, if asked, the grounds supporting that reason.

Inland Revenue may also decide to:

- release the information subject to certain conditions (for an OIA)
- release the information with an additional statement to put it into context (this can be useful if there is a concern that releasing the requested information on its own might be misleading or incomplete), and
- release other additional information we consider relevant to the request and helpful to the requester.

If the information to be released is contained in a document that includes other information outside the scope of the request, Inland Revenue can choose to:

- release the document in its entirety, or
- delete the information that is outside the scope of the request and advise the requester accordingly.

If deleting information as being outside the scope of the request, it is important not to take an unreasonably narrow interpretation of the request.

However the information is released, we should keep a replica of that information, as any decision to withhold official information can be reviewed by either the ombudsman or by an internal review. It is important to keep clear and accurate records of what has been released or withheld and why.

Tips for making deletions

Deletions (redactions) can be made by:

- whiting out the information and then photocopying it
- cutting out the information and then photocopying it, or
- deleting the information electronically by using redaction software.

Alternatively, if there will be so many deletions that only a few sentences are visible on a page, consider providing a summary. This should be an accurate summary of what was requested and can be pasted into a new document.

Care should be taken with electronic releases, having regard to potentially embedded information such as document versions, track changes and pivot tables. Similarly, information should not be blacked out on a hard copy document and then photocopied, as this may **not** obscure the deleted information in certain circumstances.

Any deletions should not change the essential formatting of the document, and it is good practice to indicate the reasons for the deletions on the document itself.

Screen dumps
It is no longer necessary to redact user ID, screen-system ID and screen identifier information from system screenshots.

Analyse the information

Analyse the material gathered to see whether any information can be released. There are times when personal information about a requester would not be given to them. For example:

- once Inland Revenue has advised that a tax investigation is to commence and disclosure would prejudice the effective conduct of the investigation
- when the information requested would disclose the identity of a person who has supplied information to Inland Revenue, thereby breaching an obligation of confidentiality, and
- when the information requested would disclose particular targeting or investigation techniques and selection criteria which, if disclosed, would prejudice Inland Revenue's ability to investigate in the future.

In these cases, a request maybe refused as the release of this information would be likely to prejudice the maintenance of the law.

If you have any doubts about anything, check them out with the appropriate people, i.e. subject matter experts, LTS, the Privacy Officer or Government and Executive Services.

Common withholding provisions in the OIA

It is important to understand the scope of a request to correctly apply the withholding provisions. To do this, you will need to analyse each individual item of information and consider whether to withhold any information based on the withholding criteria. Making a "blanket approach" does not comply with the Act. The *Kelsey* case (explained below) emphasises the importance of scope and understanding the correct application of the withholding provisions.

The *Kelsey* case (*Kelsey v Minister of Trade [2016] 2 NZLR 218*) is a useful reminder that officials should not take blanket approaches to withholding information and should read the relevant documents to consider whether any information can be released. The case also emphasises that, when applying the substantial collation and research withholding ground, officials must first consider whether to extend the timeframe response or charge for their time. The case related to decisions made purely under the OIA where the principle of availability of information applies (whereas Inland Revenue has the opposite starting point under the TAA). However, the *Kelsey* case still makes the useful point that we need to have a good understanding of the information that falls within scope of a request in order to be able to justify our use of withholding grounds.

You will need to establish if the information requested is subject to tax confidentiality under section 18 of the TAA (in most cases, information **will** be tax confidential). The second step is to establish whether any of the exceptions to confidentiality apply (that is, a "permitted disclosure", as noted above). If none of the exceptions apply, you can withhold under section 18(c)(i) of the OIA:

> The information you requested is refused under section 18(c)(i) of the OIA as making the requested information available would be contrary to the provisions of a specified enactment, namely Inland Revenue's confidentiality obligation in section 18 of the Tax Administration Act 1994 (TAA). Disclosing the information requested does not fall within any of the exceptions to the confidentiality obligation in section 18 of the TAA.

If the information requested is not tax confidential , consider whether any of the following commonly used withholding grounds apply:

Consideration	**OIA reference**
The release could prejudice the maintenance of the law.	section 6(c) – disclosure would prejudice the maintenance of the law.
The release would provide personal information about other individuals.	section 9(2)(a) – to protect the privacy of natural persons, including deceased persons.
The release could compromise the commercial position of the person who supplied or is the subject of the information.	section 9(2)(b)(ii) – to protect the commercial position of the person who supplied the information or who is the subject of the information.

The release would breach the confidentiality of advice tendered by, or to Ministers of the Crown and officials.	section 9(2)(f)(iv) – to maintain the current constitutional conventions protecting the confidentiality of advice tendered by Ministers and officials.
The release would prevent the free and frank expressions of opinions.	section 9(2)(g)(i) – to maintain the effective conduct of public affairs through the free and frank expressions of opinion.
An administrative reason for refusing a request for information.	section 18(d) – the information requested is or will soon be publicly available.
We can't be sure the information exists, or know where it is.	section 18(e) – the document alleged to contain the information requested does not exist or cannot be found *[note that you should check section 18B if you intend to withhold information under section 18(e)].*
The release requires substantial collation or research.	section 18(f) – the information requested cannot be made *available without substantial collation or research [note that you check section 18A and 18B if you intend to withhold information under section 18(f)].*

Common withholding provisions under the PA

Section 18G of the TAA permits Inland Revenue to provide people (or their representative) with sensitive revenue information. Clause 15 of schedule 7 of the TAA sets out to caveats on provision of the personal information. The Commissioner must consider whether –

- the information is readily available; and
- if it is "reasonable and practical" to provide the information.

Inland Revenue is subject to the information privacy principles in the PA. Principle 6 provides that where an agency holds personal information in a form that is readily retrievable, individuals are entitled to have access to information relating to them.

If we consider that the disclosure of the information would adversely affect the integrity of the tax system. Although the information may be personal information, there would not be a permitted disclosure as it would not be "reasonable and practical" for the Commissioner to disclose the information.

Before releasing information in response to a request under the Privacy Act consider whether any of the reasons for refusal to supply information are contained in sections 27, 28 and 29 of the PA are applicable in the circumstances.

Consideration	**PA reference**
The release could prejudice the maintenance of the law including the detection, investigation or prosecution of offences.	section 27(1)(c) [note this can be used if there is a current investigation, but generally not if the investigation has been completed]. It can also be used to withhold the names of informants.
The release is likely to put a person in danger.	section 27(1)(d) [note this must be physical safety and you must have evidence to prove the danger].

The release would provide personal information about other individuals.	section 29(1)(a) An agency may refuse to disclose any information requested under principle 6 if disclosing the information would involve the unwarranted disclosure of the affairs of another individual or a deceased individual. [note this may be used to remove staff names in some circumstances but if staff have had direct contact with the requester there would be no reason to delete their name
The information requested is evaluative material and disclosing the information, or information identifying the person who supplied it, would breach a promise made to that person that the information, or their identity, would be held in confidence.	section 29(1)(b) [note evaluative material is very specific and only applies to evaluative or opinion material compiled solely to determine someone's suitability, eligibility or qualifications for employment, appointment, promotion or removal from employment];
Disclosure of the information would breach legal professional privilege;	section 29(1)(f)

The information requested is not readily retrievable.	section 29(2)(a)
The information does not exist or cannot be found	section 29(2)(b)
The information requested is not held by Inland Revenue and the person dealing with the request has no grounds for believing the information is held by another agency.	section 29(2)(c)

Communicating the decision

A decision on the request must be communicated by giving or posting notice to the requester within the relevant timeframe.

Notice of the decision must include:

- whether the request will be granted, and if so
- in what manner, and
- for what charge (if any) if an OIA request (you cannot charge for responding to a PA request).

Decisions should be clearly worded and sensitive to any particular needs the requester may have.

If the decision is to **refuse** the request, reasons must be given for that decision. This means that you must refer to the particular subsection relied on under the OIA or PA (as applicable) to refuse the request.

The OIA also requires agencies to provide the grounds for relying on the relevant subsection, if the requester asks for them.

Every decision to refuse a request must advise the requester of the right to complain to the Ombudsman or the Privacy Commissioner (as applicable) and to seek an investigation and review of Inland Revenue's decision. Refer to the template letter(s) for communicating a decision to the requester.

The requester also has the option of seeking a review on OIA decisions by an Inland Revenue officer. This option doesn't preclude the requester seeking a review by the Ombudsman if the requester is not satisfied with the department's internal review.

Releasing information in response to a request

The OIA requires that information must be made available without *"undue delay"*. Generally, when a decision is made to grant a request for information, whether in full or in part, the decision and the information should be provided to the requester at the same time.

However, there may be times when this is not possible. For example, when the request is for a large amount of information and although Inland Revenue has reached a decision to grant the request, it will still take further time to prepare the information for release.

Provided that there is no undue delay, the information may be provided to the requester at a later stage, after the decision has been made and communicated. In these circumstances, the notice of the decision should clearly indicate that the information will be provided, with an estimated timeframe for the release. If some of the information is to be withheld, the notice should also advise this and state the reasons for refusing that part of the request.

A later release of information may also be appropriate when a decision has been made to charge for providing the information. Inland Revenue may require all or part payment of the charge in advance, before the work is undertaken to prepare the information for release. (See the "Charging" section below.)

Awaiting the requester's response to know if they are prepared to be charged for the information will not generally be considered to be an undue delay in making the information available.

Complaints: OIA

Complaints about OIA decisions

Requesters have the option of raising any concerns about their OIA decision with the Office of the Ombudsman (www.ombudsman.parliament.nz) or by applying for an Inland Revenue internal review (by emailing oia@ird.govt.nz).

Inland Revenue's internal review is an independent review carried out by Government and Executive Services.

Complaints: Privacy

Complaints about PA decisions

Requesters who have concerns about their PA decisions should contact the Privacy Commissioner to seek resolution (www.privacy.org.nz).

Charging

Public sector agencies cannot charge for responding to a Privacy Act request.

Part of making a decision on a request under the OIA includes whether to charge. Any decision to charge must be notified to the requester at the same time as the requester is advised of the decision to release information, of:

- the decision to charge
- the maximum amount of the charge
- how the charge has been calculated
- whether all or part payment of the charge is required in advance of release of the information, and
- that the requester has the right to complain to the Ombudsman about the decision to charge.

Charges can be made for making the information available, including time spent retrieving and collating the information, and preparing it for release. However, charges **cannot** be made for the time spent or any expenses incurred in deciding whether or not to release the information.

It may not be reasonable to charge for locating or retrieving information if there are poor record-keeping practices in place that mean the information is not stored where it should be (in accordance with Inland Revenue's normal business practice).

The Ombudsman has published *Charging: A Guide to charging for official information under the OIA and LGOIMA*. You can access the publication here, or go to www.ombudsman.parliament.nz and look under "Resources and publications" and "Guides".

Special categories of official information

Certain rules apply to three particular categories of information that may be requested under the OIA. These are:

- internal rules or guidelines for decision making
- statements of reasons for decisions, and
- personal information requests by corporate entities.

The OIA provides requesters with a **right** to access any document which:

> *... contains policies, principles, rules, or guidelines in accordance with which decisions or recommendations are made in respect of any person or body of persons in [their] personal capacity.*

The ability to refuse such a request is very limited.

Requests for statements of reasons

Section 23 of the OIA also provides a **right** to a written statement of reasons for a decision or recommendation made about the requester by the agency.

Requests for written statements of reasons are often made by individuals or groups with concerns about a decision or recommendation that affects them personally. The right to a statement of reasons provides a requester with the ability to obtain further information about that decision.

Requesters need not specifically refer to section 23 of the OIA in seeking to invoke their right to request a written statement of reasons for a decision that has affected them personally. However, it should be relatively clear from the terms of the request that this is what they are seeking to obtain. If it is unclear whether the requester is seeking a written statement of reasons, it may help to consult them.

The right to request for a written statement of reasons must be exercised within a *'reasonable time'* of the decision or recommendation at issue.

A written statement of reasons should be full and comprehensive in explaining the decision making process, and must include the following elements:

- the findings on material issues of fact
- a reference to the information on which the findings were based, and
- the reasons for the decision or recommendation.

Inland Revenue may already hold a written statement that contains all the elements listed above. If not, we will need to create such a statement.

There is only a limited basis to withhold information from a statement of reasons (see sections 23(1), 23 (2A) and 23 (2B) of the OIA).

Information requests by corporate entities

Every corporate entity (company or incorporated society), which is either incorporated in New Zealand or has a place of business in New Zealand, has the **right** to access any information an agency holds about it, under section 24 of the OIA.

The requirements for Inland Revenue to process such requests are more or less the same as for any other request for official information. However, as the corporate entity has a specific right to access any information about itself that can be readily retrieved, the reasons for refusing such requests are more limited. Section 24 of the OIA is subject to section 52 of the OIA, which makes it clear that such reasons may include that the information is subject to tax confidentiality obligations under the TAA and no exception to secrecy applies.

Special precautions must also be taken when information is released, to confirm the identity of the requester and ensure that the information will only be received by the requester or their authorised agent. The requester must also be advised of their right to request correction of the information released.

Conditional release

The OIA implicitly recognises that information may be released subject to conditions on the use, communication or publication of the information. Conditions can include:

- an embargo
- a requirement that the requester keep the information confidential
- a requirement that any discussion of the information should include reference to a contextual statement the agency has also provided, and
- a requirement to use the information only for a specific purpose.

It is important to note that conditions are **not enforceable** under the OIA. Releasing information subject to a condition therefore relies on a relationship of trust and confidence between the agency and the requester, or the establishment of a formal contract or deed.

You cannot place conditions on the use of information released under the Privacy Act.

Publication of information

An agency may, whether proactively or in response to a request, choose to publish information as it sees fit. For example, an agency may decide to make information generally available to the public on its website.

Proactively releasing information to the public promotes good government, openness and transparency and fosters public trust and confidence in agencies. Proactively releasing information also has administrative benefits for the agency, including by reducing requests for information which is already publicly available, and allowing for greater ease of handling of the requests that are received.

Note that responses to requests made via the FYI website www.fyi.org.nz are published online on that site.

Good faith protection

Occasionally, an agency may be reluctant to make official information available for fear that release of the information could expose the agency to litigation.

However, releasing information in good faith in response to a request made under the OIA will not expose an agency to civil or criminal proceedings. The OIA explicitly states:

> *Where any official information is made available in good faith pursuant to this Act no proceedings, civil or criminal, shall lie against the Crown or any other person in respect of the making available of that information, or for any consequences that follow ….*

This means that, as long as an agency releases information in the honest belief that the OIA requires disclosure (which may be demonstrated by the agency having made reasonable efforts to identify the interests requiring protection as well as any public interest in release, and to consider those interests in good faith), no civil or criminal proceedings will lie against the agency. This section effectively protects the Crown from any defamation or breach of confidence proceedings, or complaints to the Privacy Commissioner under the Privacy Act, in respect of information which is made available in good faith under the OIA.

Some protection is also afforded to the author or supplier of the information. However, such protection does not extend to publication of the information by the requester or subsequent parties, such as a newspaper.

The good faith protection under the OIA is also not available when an agency decides to proactively release information, rather than releasing information to a requester in response to an OIA request.

Even when an agency does release information in good faith under the OIA, a complaint to the Ombudsman under the OA may still be made by any person affected by the release, if it is considered that the agency has not acted in an administratively reasonable manner. For example, by not taking due care when making deletions to information, or not affording them a reasonable opportunity to comment before release.

Further guidance from the Ombudsman

Separate guidance is available on making a decision whether or not to grant a request, in relation to particular sections of the OIA and specific subject areas.

The Ombudsman's website contains searchable case notes, opinions and other material relating to past cases considered by the Ombudsman: www.ombudsman.parliament.nz.

The Ombudsman's staff can provide general advice to agencies on the processing of an official information request, including the current interpretation of the OIA and how it has been applied in similar fact situations in the past. You can email info@ombudsman.parliament.nz or freephone 0800 802 602.

Appendix

Process for responding to straightforward information requests: eight steps

Once you have decided that Inland Revenue holds the information requested, and you have determined which Act(s) applies (TAA, OIA or PA), the following steps must always occur:

1) Identify the information you need to respond to the request, or if it should be transferred to another agency

2) Develop your timeline

3) Find the documents

4) Analyse and consult

5) Update records

6) Decide if you need to extend the time limit

7) Draft the response

8) Get the sign-off, send the response and update records

Identify the information you need to respond to the request

Scope the response: read the request carefully and identify anything that seems unclear. If there is any ambiguity, consider consulting with the requester to clarify exactly what they are requesting. Think about the context of the request and what the requester may want to know, and why. This may help identify things that the requester may not need or want to receive. Clarifying a request will save time and effort in the long run.

Develop your timeline

The statutory deadline for a response is 20 working days from when Inland Revenue (not the relevant business unit) receives a request. A tool that automatically calculates the statutory due dates for responses to information requests is available on the Ombudsman's website at www.ombudsman.parliament.nz. You find information about OIA requests and access the Ombudsman's time calculator via the Stakeholder Relations intranet page.

Once you have the final 20-day deadline, work backwards to calculate your timeline – for example, how long you can take to compile the information, when you will need to finish drafting your response by, and when it will need to be approved by a manager. It's very helpful to leave a buffer of at least two days, as some steps take longer than expected.

Be aware that some steps in the process affect each other, so you may need to keep adjusting your timeline (this is also where the buffer comes in handy). The statutory deadline is 20 working days from when the request is received, but Inland Revenue's obligation is to respond as soon as reasonably practicable. So if we can respond to a request before the maximum statutory time limit, we should.

Find the documents

If the requester is asking for various types of information or complex data, identify and consult with key staff who are likely to know what information exists and where it might be held, including access to other system or databases, to gather the requested information. Keep a record of your searches. In the event that no relevant information can be found, it's helpful to be able show that all reasonable efforts were made to locate the information (especially in the case of a complaint to the Ombudsman about our response).

Analyse and consult

Analyse the material gathered to see whether any information can be released.

There are times when even personal information about a requester cannot be released to them:

- once Inland Revenue has advised that a tax investigation is to commence and disclosure would prejudice the effective conduct of the investigation
- when the information requested would disclose the identity of a person who has supplied information to Inland Revenue, thereby breaching an obligation of confidentiality, or
- when the information requested would disclose particular targeting or investigation techniques and selection criteria which, if disclosed, would prejudice Inland Revenue's ability to investigate in the future.

In these cases, a request can be refused under 6(c) of the OIA, as the release of this information would likely to prejudice the maintenance of the law.

If you have any doubts about anything check it out with the appropriate people. For example: subject-matter experts, LTS, Inland Revenue's Privacy Officer, or Government and Executive Services.

Keep records

Any decision to withhold official information can be reviewed by the Ombudsman or by an internal review. It is therefore important to keep clear and accurate records of what has been released or withheld and why.

When preparing documents that will have information redacted (withheld), make three copies of each document: a clean copy, a mark-up copy (that shows which parts of the document will be withheld or released and why), and the final, redacted copy (with information blacked out). The redacted copy will be sent to the requester.

It is no longer necessary to redact user ID, screen-system ID and screen identifier information from system screenshots.

Decide if you need to extend the time limit

If extensive retrieval of documents or consultations necessary to make a decision are making the 20-day time limit unachievable, you can extend the time limit to respond to a request. You can extend the time limit at any point before the original 20 days end.

However, unless it is obvious at the start, it's best practice not to extend until you have already, in good faith, tried to answer the request. This way, you will have a good idea of how long to extend the time.

If you need to extend the time limit, you must advise the requester of the period of the extension (which must be reasonable, for example five or ten working days) and give the reasons for the extension.

Under the OIA, the only acceptable reasons for extending the time limit are:

- the request is for a large quantity of information or necessitates a search through a large quantity of information, and meeting the original time limit would unreasonably interfere with the operations of Inland Revenue; or
- consultations necessary to make a decision on the request are such that a proper response to the request cannot reasonably be made within the original time limit.

In all other cases, Inland Revenue must keep to the statutory deadline.

Get the sign-off, send the response and update records

Remember to check that you know who in your area has the revenue delegation to sign the response. This means they have the approval to authorise the release or withholding of information. It's a good idea to include in your records the position or title of the person who holds the revenue delegation and has approved the response.

This is an added protection for Inland Revenue. In the past, people have signed out responses without having the appropriate delegation to do so.

Troubleshooting tips

A number of factors can contribute to delays and administrative difficulties in processing an OIA or PA request. Most of these factors are addressed in this guide or on the Ombudsman's website at www.ombudsman.parliament.nz

Consulting the requester

If you need to consult the requester, do so as soon as possible. If you consult within the first seven working days of the request, it may be possible to treat any amended or clarified request as a new request (see the "Amended or clarified requests" section).

If you need to consult the requester, it may really help you to collate the information if you ask them:

- to be as clear and specific as possible about the information they want, and
- if there's any information they don't want.

These points may also be helpful:

- If the requester is seeking reasons why a decision or recommendation was made: the request may be for a statement of reasons under section 23 rather than for documentary information.
- If a requester has asked for urgent consideration, it's reasonable to ask why it's urgent and for their timeframe. (The Ombudsman's view is that agencies should consider requests for urgency, but do not have to treat the request as such.)
- If you need to consult third parties before making a decision on the request, ask the requester if they have concerns with the disclosure of their identity to third

parties. (If they do have concerns, we can consult without revealing the requester's identity).

- If there's a lot of information or the requester has asked for it to be provided in a format that's difficult to do, you can ask if they would be happy to receive the information in an alternative form that would be easier to provide (e.g. an oral briefing, a viewing, or a summary of the information).

Taking ownership to co-ordinate and manage a broad or multi-revenue detailed request

Inland Revenue often receives requests that are very broad. For example, a customer might request information that covers a wide range of information including multiple tax types (child support and income tax), and that covers a long period of time.

If this is the case:

- First, ascertain if this request meets the criteria to be managed by Government and Executive Services. If not, then:
- Establish who will take overall responsibility and ownership of the request.
- If you are responding to the request identify who else needs to be involved in considering the request to supply the information.
- Arrange a scoping meeting with these identified people to verify if the requester has previously made similar requests or if there are any investigations or legal cases underway.
- To avoid multiple contacts about different aspects of the request by various Inland Revenue people, nominate one person to make contact with the customer.
- Explain the problem, including how much information their request covers as currently phrased.
- Invite the requester to reconsider or refine their request. If you take steps to consult the requester within the first seven working days, it may be possible to treat any amended or clarified request that is received as a new request (see amended or clarified requests above). Have in mind some potential strategies for refining or redirecting the request that might be able to meet the needs of the requester without imposing an unreasonable administrative burden on Inland Revenue. For instance:
    - Refining the time period covered by the request.
    - Refining the types of document covered by the request.
    - Consider engaging additional staff.
    - Consider whether charging for the supply of information would be reasonable and appropriate in the circumstances.
    - Consider whether to extend the maximum time limit for making a decision on the request.
    - Consider whether it is possible to release the information in an alternative form, for example, summarised.
    - Consider releasing the information at a later time, after the decision is made, as long as the information is prepared for release without undue delay.
    - As a last resort, the decision maker who holds the appropriate delegation may need to consider whether it is necessary for Inland Revenue to refuse the request under section 18(f) of the OIA, on the basis that the

information cannot be made available without substantial collation or research.

Managing multiple requests from the same requester

- Invite the requester to prioritise the order in which they would prefer the requests to be answered.
- Consider extending the time limit on each request as needed.
- Consider whether charging for the supply of information would be reasonable and appropriate in the circumstances.
- Advise the requester of the decision on each request as soon as reasonably practicable (and no later than 20 working days), and subsequently roll out the information to be released without undue delay.
- Consider whether it is possible to release the information in an alternative form, for example, summary, viewing, or oral briefing.
- Consider whether, in the circumstances of the case, the multiple requests can be treated as a single request under section 18A(2) of the OIA, for the purposes of deciding whether it is appropriate to refuse the request under section 18(f) on the basis that the information cannot be made available without substantial collation or research.
- Consider whether it would be appropriate to refuse the requests under section 18(h) on the grounds that the requests are frivolous or vexatious.

What to do when the information requested is difficult to identify or cannot be found

- Contact the requester—explain the problem and ask whether the request can be made more specific, or whether they can provide more information to assist in locating the information.
- Consider whether Inland Revenue is being asked to create information or express an opinion rather than to provide information that it holds.
- If the information is in the form of discussions that were held but not recorded, identify the relevant officials and record their recollections in writing.
- Consider extending the time limit to give Inland Revenue more time to locate the information.
- Consider whether all or part of the request should be transferred to another agency that does hold the information.
- Consider whether it is appropriate to refuse the request under section 18(e) of the OIA on the basis that the relevant document does not exist or cannot be found, despite reasonable efforts to locate it.
- Consider whether it is appropriate to refuse the request under section 18(g) of the OIA on the basis that the agency does not hold the information and has no grounds for believing the information is held by, or more closely connected with the functions of, another agency subject to the OIA or LGOIMA.

What to do when the information is not ready to be released

- Consider refusing the request under section 18(d) of the OIA, if the information will soon be publicly available (for example the information is being printed or is in the final stages of being prepared for imminent public release). If so, explain to the requester:
    - where and how the information will be able to be obtained;
    - the date of public release; and
    - the difficulty in meeting the request immediately.
- Consider whether there is a substantive concern about releasing the information at the time of the request. If so, identify the particular harm in release at this stage and assess that harm against the reasons in the OIA for withholding information.

Revenue delegations

Under section 7 of the Tax Administration Act 1994, the Commissioner of Inland Revenue has the authority to delegate functions or powers of the Commissioner, to Inland Revenue employees under any of the Inland Revenue Acts.

The purpose of these delegations is to enable you to make decisions that are delegated to you under the appropriate Inland Revenue Act and that relate to your day to day work in the position you currently hold taking into account an assessment of your level of skills and experience you have displayed.

Delegations fall under three main areas of responsibility:

- revenue
- financial, or
- human resources.

Your delegation letter sets out the authority levels you have under those three areas of delegations. Check your delegation letter to identify your Business Group and Position.

The Business Group is the group you currently work for, and your current position title for which these delegations apply.

Example:

Your Business Group is Customer Services, identified on the matrix as **Group K**
Your position title is: Customer Service Specialist, Fundamental/Applied – position identifier in the matrix as **CSSFA.**

<u>Revenue Delegations</u>

The Acts for which you have revenue delegations are:

(Example:)

• Income Tax Acts 1994, 2004 and 2007
• Tax Administration Act 1994

• Goods and Services Tax Act 1985
• Child Support Act 1991
• Student Loan Scheme Act 2011
• KiwiSaver Act 2006

The specific provisions within the Acts that you are delegated to make tax technical decisions under can be found in the Revenue delegations matrix.

This guide may be helpful: **How to find what you are looking for in the Revenue delegation matrix**

OIA training: Summary

The Official Information Act 1982:
What it is, what it does and how to use it

For a more detailed guide, see the *OIA training: Full guide*

Acts of law

Inland Revenue is subject to the Tax Administration Act (TAA), the Official Information Act (OIA) and Privacy Act (PA). These Acts impose requirements on how we deal with requests for information.

Official Information Act

The Official Information Act 1982 provides a general public right of access to official information. The purpose of the OIA is to facilitate open government, and therefore the presumption is that government agencies will be as open as possible.

Privacy Act

The Privacy Act 1993 gives individuals a right to access personal information about themselves that is held by an agency. Personal information about an entity that is not a natural person is considered under the OIA. The Privacy Act 2020 will come into force on 1 December 2020.

Tax Administration Act

Under the Tax Administration Act 1994, the Commissioner of Inland Revenue has an obligation to maintain confidentiality in relation to sensitive revenue information, and is not required to disclose information that would adversely affect the integrity of the tax system or the maintenance of the law.

The general right of access under the OIA, and the individual's right to personal information under the PA, are both subject to the confidentiality provisions of the TAA.

Unless otherwise stated, legislation in this guide refers to the OIA.

In a hurry? Go straight to the summary.

Examples of wording you can use are here.

Need help with an OIA?

That's what we're here for! Contact GES @ MinisterialServices@ird.govt.nz

Contents

        - Sensitive revenue information
        - Aggregate and statistical information
        - Flowchart: revenue or sensitive revenue information?
        - Integrity of the tax system and maintenance of the law
        - Contrary to legislation – section 18(c)(i) of the OIA
            - Audit and investigative techniques
            - Police investigations
        - Permitted disclosures of sensitive revenue information
            - Carrying into effect a revenue law – section 18D(1)
            - Carrying out or supporting a function of the CIR – section 18D(2)
    - Security, defence or international relations of New Zealand – section 6(a) of the OIA
    - Information entrusted by another country – section 6(b)
    - Prejudice the safety of any person – section 6(d)
    - The request is frivolous, vexatious or trivial – section 18(g)
- Examples

Summary

More information about each point is in the next section.

Examples of wording are in the *Examples* section at the end of this guide.

Statutory deadline – Official Information Act requests (OIAs) have a statutory deadline, which means Inland Revenue **must** respond by the due date. The statutory deadline is 20 working days from the working day after we receive the request. The Ombudsman has a handy online OIA response calculator at www.ombudsman.parliament.nz.

Rights of review – A requestor can complain to the Ombudsman and ask for an investigation into our decision on their OIA request. Requestors can also ask us for an internal review of the OIA decision.

Making a decision on the request – The statutory deadline is the date by which you must make a decision on the request, not necessarily to provide the information. If you know you can release the information, but it will take longer to retrieve or collate, reply by or before the deadline with your decision and the date by which you will provide the information. If you need more time to decide, consider if you can extend the timeframe.

Clarifying a request – If you ask the requestor to amend or clarify their request within 7 working days of us receiving the request, the amended/clarified request may be treated as a new request. This resets the timeframe to 20 days from the date the requestor responds. If you ask for clarification after 7 days, the original deadline will apply.

Transferring a request – You can transfer a request to another agency if they have the information requested, but you must transfer within 10 days.

Extending a request – You can extend a request for a reasonable amount of time, e.g. 10 working days, but only for specific reasons.

Inform the requestor – Whatever you're doing with a request: responding, extending or transferring, you must let the requestor know by the original statutory deadline.

Releasing all information – If there is no reason to refuse the information, release it.

Tax confidentiality and sensitive revenue information – Is the information requested sensitive revenue information and therefore confidential under s.18 of the TAA? If so, you can refuse it, as the TAA takes precedence over the OIA (and PA).

Aggregate and statistical data is not sensitive revenue information, so can usually be released.

Refusing information – The OIA allows refusals, but only for specific reasons. The most common refusal grounds are in the following table. For more reasons and more details, see *Refusing information* in the next section.

Table of common reasons for needing to refuse the information

Reason for needing to refuse the information	**Refuse under this section of the OIA**
to protect personal privacy (of staff or customers)	9(2)(a)
the information is already publicly available or soon* will be	18(d)
the information is sensitive revenue information and therefore confidential under the TAA**	18(c)(i) of the OIA (contrary to legislation), because it is contrary to s.18(1) of the TAA.
the information does not exist or cannot be found	18(e)
the information is not held	18(g)
release would require substantial collation and research***	18(f)
the information is confidential	9(2)(ba)
the request is frivolous, vexatious or trivial	18(h)
refusing is necessary to protect the politically neutrality of officials	9(2)(f)(iii)
refusing is necessary to protect the confidentiality of advice tendered by officials to the Minister	9(2)(f)(iv)
refusing is necessary to protect the free and frank, and effective conduct of government	9(2)(g)(ii)
refusing is necessary to protect legal professional privilege	9(2)(h)
refusing is necessary to protect commercial prejudice	9(2)(b)

* "Soon" is about eight weeks after the statutory deadline.

** If information is not sensitive revenue information but is revenue information, you may be able to release it. Some sensitive revenue information can be released if certain exceptions are met.

*** Before using the substantial collation and research section, s.18(f), first consider if you could provide the information if: the requestor refined their request; or you extended the time limit; or you imposed a charge for providing the information (there are set amounts). Wait for the requestor to agree to the charge before you go ahead with collating the information.

A full list of all the possible refusal grounds is here.

What is official information?

All information held by Inland Revenue is official information.

However, official information is not limited to documents. It includes information in **any format**, such as:

- Written documents including reports, drafts, letters, notes, emails, eCase notes and attachments, text messages and messages sent via apps.
- Non-written documentary information such as material stored on or generated by computers, including databases, video or audio recordings e.g. recordings and transcripts created in Teams.
- Information that is known to Inland Revenue, but which has not yet been recorded in writing or otherwise (including knowledge of a particular matter held by an officer, employee or member of Inland Revenue in their official capacity).
- Documents and manuals that set out the policies, principles, rules or guidelines for decision-making by Inland Revenue.
- The reasons for any decisions that have been made about a person.

Inland Revenue's obligations under the OIA

Principle of availability

Requested information should be made available unless there is good reason to withhold it under the OIA.

Deadline for responding to an OIA request

We **must** respond to an OIA request by or before the statutory deadline. Don't wait until the day of the deadline if you can respond earlier. Under the OIA, agencies have an obligation to respond "as soon as reasonably practicable".

It's best to use the Office of the Ombudsman's online OIA response calculator. Type in the date you received an OIA request and it will give you the deadline for responding to the request. This is a statutory deadline, so we **must** respond by this date. The calculator is on the Ombudsman's website: www.ombudsman.parliament.nz

To work out the deadline, count 20 working days from the day after you received the request. Weekends and national public holidays are not working days. Local holidays, such as anniversary days, are counted as working days.

A working day is a weekday and finishes at midnight. So, whether a request is received on 10am or 10pm on a Monday, it's still received on Monday. Equally, whether we send a response on a Monday before or after 5pm, it's still sent on Monday.

For the OIA to apply, the information must be held by Inland Revenue at the time the request is received. Apart from providing a response to a request for a statement of reasons, there is **no obligation on Inland Revenue to form an opinion or create information** to answer a request.

There is a difference between a requestor asking:

- questions that can be answered by providing information already known to and held by Inland Revenue (official information), and
- questions that require Inland Revenue to form an opinion or provide an explanation and so create new information to answer the request (not official information).

If a request is made for information that is **not** held by Inland Revenue, consider:

- transferring the request to another agency subject to the OIA or the Local Government Official Information and Meeting Act 1987 (LGOIMA), or
- refusing the request under sections 18(e) or 18(g) of the OIA (because the requested document does not exist, or the information is not held).

Creating information

Inland Revenue may choose to create information to respond to a request. We are **not** required to create information in order to answer a request.

See advice about refusing requests under section 18(e) of the OIA, because the information does not exist or cannot be found.

However, if the information would be easy to create, consider if it could be seen as unreasonable for Inland Revenue to refuse to do so. Under the Ombudsmen Act 1975, a requestor can complain to the Ombudsman about our response.

Provide a decision within 20 days

A decision whether to grant a request or charge for a request must be made and communicated to a requestor "as soon as reasonably practical" and no later than 20 working days after the day on which the request was received. Ref section 15(1) of the OIA. The decision on a request can be to:

- release
- refuse
- extend, or
- impose a charge.

Failure to meet the 20 working-day deadline

The request is deemed to be refused if the statutory deadline is not met (a delay is deemed a refusal). The requestor may make a complaint to the Ombudsman.

Transfer a request within 10 days

Under section 14 of the OIA, if you need to transfer an OIA request to another agency, you must transfer the request within 10 working days. We need to write to the requestor to advise them of the transfer, and also to the agency we're transferring the request to. Remember to send the agency the request and the requestor's contact details.

First, ensure the information is held by the other agency

When transferring a request because another agency is more closely connected to the information, first ensure that the other agency does hold all the information in scope of the request.

If there is some information Inland Revenue holds that the other agency does not hold, we should transfer the part of the request we cannot answer and respond to the part of the request we can answer.

The other agency will have 20 working days to respond to the OIA from the date they receive our transferred request.

Similarly, when another agency transfers an OIA request they have received to Inland Revenue, the 20 working days begin from the date we receive the transferred request.

Advice about Ministers and transfers is here.

Clarify a request within 7 days and reset the day count

If Inland Revenue seeks to amend or clarify the request within 7 working days of us receiving the request, the amended/clarified request may be treated as a new request that replaces the original request. Under s.15(1AA) of the OIA, we can reset the timeframe for responding to a request – but only if we have asked the requestor to clarify their request within 7 working days.

The new date will be 20 days from the date the requestor comes back with the amendment/clarification. If the requestor does not respond, we are still obliged to respond to the initial request within 20 working days, although this may result in refusal based on our interpretation of the request.

You can ask the requestor to clarify their request after seven days, but the original deadline will apply.

Extend the time to respond to the request

The 20 working-day requirement is for a **decision** to be made on a request, not for the actual information. However, the OIA specifies that the information should be released (if the decision is to release) "without undue delay".

Under section 15A of the OIA, you can extend the time to respond to a request if:

a) the request is for a lot of information or you need to search through a lot of information (and meeting the original time limit would unreasonably interfere with the operations of the department or the Minister), or

b) you need to consult in order to make a decision on the request.

"Consulting" can be discussions within Inland Revenue or with another agency.

You must let the requestor know in writing that you are extending the deadline within the original 20 working-day deadline. Let the requestor know the new extended statutory deadline for their OIA by giving a date as well as the number of working days, for clarity. You *can* extend more than once if you must, but you must send out both extensions within the original deadline.

You can extend the time for as long as you will need but keep it reasonable: 10 working days if you can (or 20 working days if you really need longer). You must respond to the request by your extended date, or this will be deemed to be a refusal of the request.

Send the response as soon as you can—don't wait until the extended deadline if it's ready before then. We still have the obligation to respond as soon as reasonably practicable.

You must let the requestor know that, under s28(3) of the OIA, they have the right to complain to the Ombudsman about the extension of time.

Extending and transferring an OIA

It's not ideal, but if you haven't realised within 10 days that you need to transfer a request (see *Transferring the request*), you can still transfer the request to the appropriate agency.

If you have to, you can extend and transfer at the same time. Quote both sections of the legislation in your response to the requestor: the extension grounds in s.15A *and* the transfer grounds in s.14(b)(ii) of the OIA.

Provide the information in the format requested

A requestor might specify that they need the information in a specific format, such as a spreadsheet. Section 16 of the OIA states that we should try to give information in the format requested if we can.

However, we don't have to give information in the format requested if doing so would impair the department's efficient administration (e.g. the requestor has asked for information to be sent on a DVD or other technology we no longer use, so it would be difficult for us to provide the information this way). In this case, we should still supply the information, but it's reasonable to do so in a format that's more convenient for us.

If you can't supply the actual information, can you release a summary? You could also consider allowing the requestor to view the document, giving them a copy of the document with redactions, or telling them what the document contains.

Right to complain to the Ombudsman

Under section 28 of the OIA, if we are refusing a request or part of a request, or have decided to charge the requestor for providing the information, we must advise the requestor of their right to make a complaint to the Ombudsman. There's an example of the wording here.

Correspondence with the Ombudsman

General correspondence with the Office of the Ombudsman that is not about an investigation is subject to the OIA.

However, correspondence with the Office of the Ombudsman that relates to an Ombudsman's investigation is not subject to the OIA, so you can withhold this without referring to any grounds.

Right to Inland Revenue review

Requestors also have the right to ask for a review of an OIA decision by someone else at Inland Revenue. It **must** be by someone else—it wouldn't be ethical for someone to review their own decision. See example wording here.

Ministers and the OIA

The OIA applies to information held by a Minister in their official capacity only.

Official information does not include information which is held by a Minister:

- in their private capacity
- in their capacity as an MP (electorate information), or
- in their capacity as a member of a political party (caucus information).

Such information may become official information if it is subsequently used for official Ministerial purposes. If this type of information is provided to Inland Revenue merely for the purpose of responding to a request for information, it is arguable that we hold the information solely as an agent on behalf of Minister.

Someone making an OIA request to a Minister has the right to complain to the Ombudsman about a decision to withhold information. However, the Minister of Revenue is not subject to a review by Inland Revenue, so only add the Ombudsman's review paragraph.

The Minister of Revenue

The current Minister of Revenue prefers to prepare his own responses to OIAs, so Inland Revenue usually transfers OIA requests for Ministerial business (such as reports the Minister has received) to his office to answer.

If you're preparing a suggested OIA response for the Minister of Revenue, the same OIA deadline and withholding grounds apply.

Ministers and transfers

The Ombudsman cannot investigate transfers under the OIA. When investigating a decision to transfer or an out-of-time transfer, this is done under the Ombudsman Act 1975. Ministers are not subject to the Ombudsman Act, so cannot be investigated for an out-of-time transfer.

Cabinet papers and the OIA

Cabinet papers must be proactively released within 30 days of Cabinet's decision on the paper. If you need to withhold some information from a Cabinet paper, you can use the OIA – just state what you're withholding and which grounds you're using.

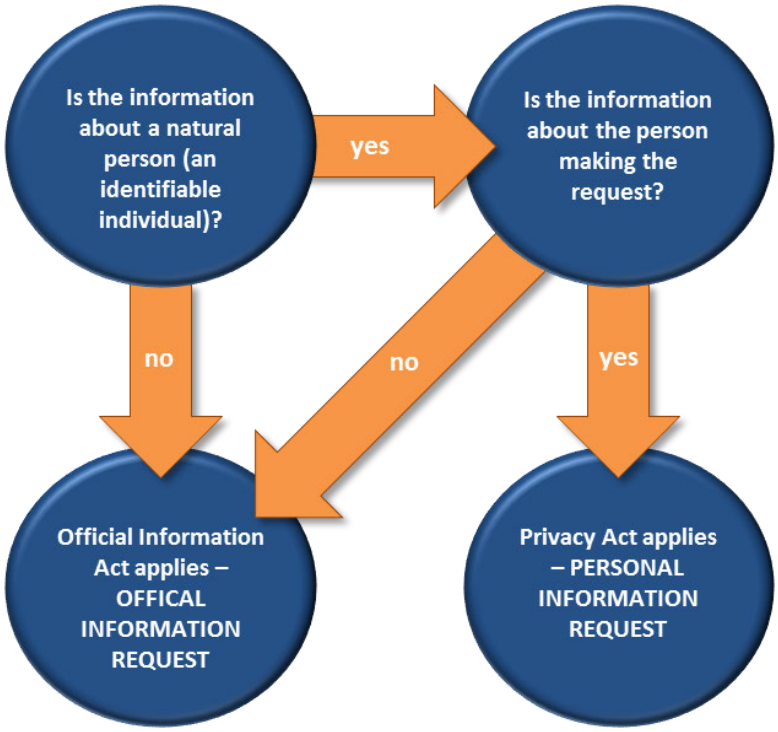
Releasing information

If you can release all the information requested, do so. You don't need to wait until the statutory deadline to respond to a request if you can respond earlier.

OIA or Privacy?

Whether the OIA or Privacy Act applies depends on who is asking for what information. When an individual asks for information about themselves, the Privacy Act applies; this includes requests from a person's authorised agent or nominated person. When the request is from someone else, or from an entity rather than a natural person, the OIA applies.

See the following flow chart:



Deleting information from documents (redactions)

A request is for each bit of information that is within scope. We are obliged to release part of a document if we can. If you can't release the whole document, release the document with the parts you can't release redacted (deleted). Provide a reason for refusing each part of the request.

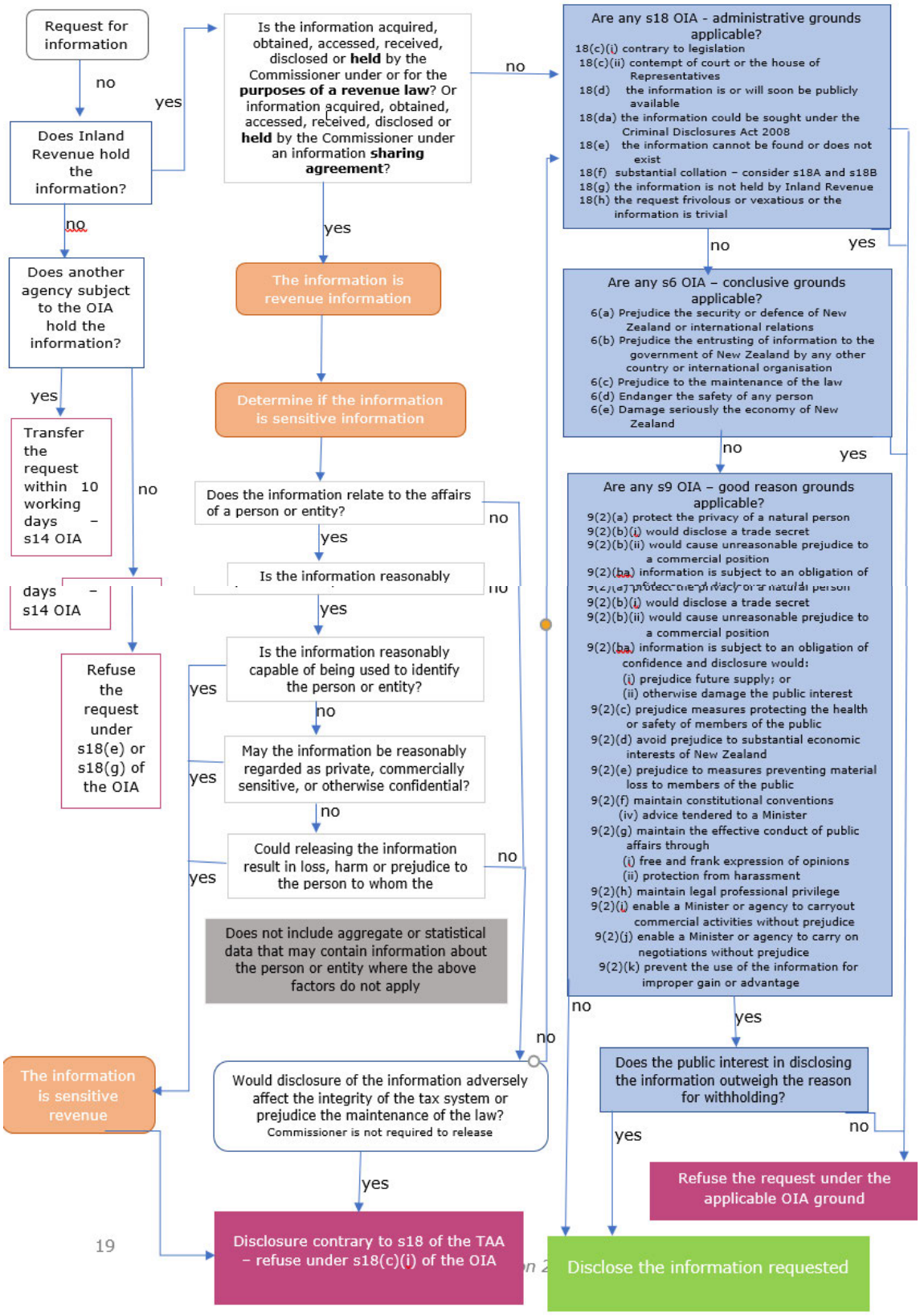
Information is out-of-date, inaccurate, incomplete or can be misinterpreted

This is not a reason for withholding. Reasonable steps should be taken to ensure that what is provided is accurate and complete. If the information is not accurate or complete, this is not a refusal reason in the OIA. We should provide the information with a contextual statement about the limitations on the accuracy or completeness of that information.

However, there may be a basis to withhold incomplete data where release would result in harm, such as commercial prejudice.

Making a decision on a request

The following flow chart summarises all our options when we receive an OIA request.



Principle of availability

Remember the principle of availability: information should be made available unless there is good reason to withhold it under the OIA, Tax Administration Act, or Privacy Act.

Public interest

If you're refusing information under section 9 of the OIA, you need to consider if your reason for refusing it is outweighed by the public interest in making the information available. See example wording here.

What is the public interest? It's broadly equivalent to the public good. This is always subjective, and has to be considered on a case-by-case basis. It can be in the public interest to have information about elections, high-profile tragedies, public spending, or finding out if government agencies have acted correctly.

Something that is interesting is not the same as being in the public interest!

If you can't supply the actual information, consider releasing a summary.

If you're refusing information under sections 6 or 18 of the OIA, you don't need to consider the public interest.

Legal privilege

Agencies can sometimes waive their legal privilege if this is outweighed by the public interest. However, Inland Revenue would have to apply to the Crown Law for permission to do so: it is not our legal privilege but the Government's.

All reasons for refusing requests

On the next page is a list of all the grounds under which a request for official information may be refused. Commonly used grounds are discussed in the following pages.

For a discussion of all the grounds, see the *OIA training – full guide*.

All refusal grounds

Administrative grounds for refusal of requests – section 18

The administrative grounds for withholding are:

- Contrary to legislation – s.18(c)(i)
- Constitutes contempt of Court or Parliament – s.18(c)(ii)
- Publicly available or soon will be – s.18(d)
- Request could be made under the Criminal Disclosures Act 2008 – s.18(da)
- Information does not exist or cannot be found – s.18(e)
- Substantial collation and research – s.18(f)
- Information not held – s.18(g)
- Request is frivolous or vexatious or the information requested is trivial – s.18(h).

Conclusive reasons for refusal of requests – section 6

The conclusive grounds for withholding are:

- Security or defence or the international relations of New Zealand – s.6(a)
- Prejudice the entrusting of information to New Zealand by another country or international organisation – s.6(b)
- Maintenance of the law – s.6(c)
- Prejudice the safety of any person – s.6(d)
- Damage the economy of New Zealand – s.6(e)
  - (i) exchange rates
  - (ii) regulation of banking
  - (iii) taxation
  - (iv) stability or control of the prices of goods and wages
  - (v) borrowing of money by the New Zealand Government
  - (vi) entering trade agreements

Other reasons for refusal of requests – section 9

These reasons must be weighed against the public interest favouring disclosure. If the public interest reasons favouring disclosure outweigh the reasons for withholding, the information should be disclosed. The section 9 grounds for withholding are:

- Privacy of a natural person – s.9(2)(a)
- Commercial prejudice - s.9(2)(b)
- Confidential - s.9(2)(ba)
- Measures protecting the health and safety of members of the public - s.9(2)(c)
- Substantial economic damage - s.9(2)(d)
- Material loss to members of the public - s.9(2)(e)
- Constitutional Conventions - s.9(2)(f)
  - (i) confidentiality of communications between the sovereign and her representative – s.9(2)(f)(i)
  - (ii) collective and individual responsibility of Ministers – s.9(2)(f)(ii)
  - (iii) politically neutrality of officials – s.9(2)(f)(iii)
  - (iv) confidentiality of advice tendered by officials to the Minister – s.9(2)(f)(iv)
- Effective conduct of government - s.9(2)(g)
  - (i) free and frank
  - (ii) harassment
- legal professional privilege – s.9(2)(h)
- Commercial activities – allow Minister or agency to carry on without prejudice – s.9(2)(i)
- Improper gain or disadvantage - s.9(2)(k)

Discussion of most used refusal grounds

Protecting a person's privacy

The OIA defines "personal information" as "any official information held about an identifiable person". Under section 9(2)(a) of the OIA, you can withhold information about natural persons if:

- the withholding of the information is necessary to "protect the privacy of natural persons, including that of deceased natural persons"; **and**
- this interest is not "outweighed by other considerations which render it desirable, in the public interest, to make that information available".

Most of the information Inland Revenue holds about taxpayers is sensitive revenue information and cannot be released under the OIA (unless an exception in section 18 of the Tax Administration Act applies).

You should refuse to provide information that identifies or could identify taxpayers, such as information about small groups of people (fewer than 10).

Personal information about staff would usually be names, phone numbers and email addresses that are in a report or email in the scope of an OIA request. **At the moment (as at 3 Nov 2020: this may soon change):** When releasing reports or emails under the OIA, Inland Revenue releases the names of staff who are managers and above, and withholds names under manager level. However, we withhold the phone numbers and email addresses of all staff.

The information is or soon will be publicly available

Under section 18(d) the OIA, you can refuse to provide information that is or soon will be publicly available. Information is publicly available if it is freely available on a website, available for purchase, available in a public library, or available for public inspection.

In these cases, refuse the information but advise the requestor where they can find it. For example, give them a website link to a document or describe how to find it online. (This would obviously be unhelpful if the requestor had advised us that they do not have easy access to the internet. In this case, it would be more appropriate to release the information and send the document.)

How soon is soon?

Before you use section 18(d), be reasonably certain that the requested information will be published soon: about eight weeks after the statutory deadline is fine.

Let the requestor know where, when, and how they will be able to obtain the information.

It's also good practise to advise the requestor once the information has been released, and to contact the requestor if there is a delay with the planned release.

The information does not exist or cannot be found

Under section 18(e) of the OIA, information may be refused if the document alleged to contain the information does not exist or cannot be found. Sometimes it can be difficult to assess whether the information should be refused because it does not exist or because it is not held (in this case you would refuse under s.18(g)).

It may be that we do hold the information on some level (e.g. in numerous forms or tax returns), but would have to create the data to provide it in the form requested. In many cases, we may choose to create the data in the form requested, in the interests of transparency and promoting voluntary compliance with the tax system. However, sometimes creating the data in the form requested would take considerable resources.

This is not a situation where we should refuse on the basis of substantial collation and research, as we would need to create the information to provide the information in the form requested. In this case, we should refuse the request under section18(e), on the basis that "the document alleged to contain the information does not exist".

Providing the information would require substantial collation or research

Under section 18(f) of the OIA, you can refuse information that would require "substantial collation or research". This term refers to the administrative difficulty in finding the information in the scope of the request, or in bringing together the requested material.

Section 18(f) may be used where there is a substantial amount of work involved in locating, extracting and collating the information in order to comply with the request, but not because of the time required in order to decide (or consult with a view to deciding) whether the information can be released.

Conditions to using 18(f)

Before you refuse on the grounds of substantial collation or research, under sections 18A and 18B of the OIA, you must consider whether doing one of the following would enable you to grant the request:

- impose a charge for providing the information
- extend the time limit for making a decision, or
- consult with the requestor to make the request more manageable.

What is collation and research, and when is it substantial?

"Research" (finding the information) and "collation" (bringing it together) includes identifying, searching for and retrieving the requested information, determining whether it is held, and assembling or compiling the requested information.

The above tasks may be considered "substantial" where they would have a significant and unreasonable impact on the agency's ability to carry out its other operations. We can also consider the resources we have available to do the work, such as the resources available to process OIA requests, the number of other OIA requests we have to deal with, the number of people capable of processing the request and, where only certain people can do the work (e.g. subject matter experts), the other responsibilities of those people.

We can also consider how much information has been requested, how much needs to be searched through to find what has been requested, how long it will take to find the information and bring it together, and who can do the work—will diversion of these people to complete the required tasks impact on IR's ability to carry out its other operations?

Alternatives to using 18(f)

There is no obligation on an agency to create information in order to respond to a request. Where the request is in the form of questions, particularly argumentative or "loaded" questions, instead of s.18(f), consider using s.18(g), the information is not held.

If the work required to complete the request is such that it amounts to the creation of new information, rather than extraction or compilation of existing information, instead of s.18(f), the relevant refusal ground to consider is also s.18(g).

The information is not held

Under section 18(g) of the OIA, you can refuse information that is not held. You can also refuse under this section where a piece of work is incomplete, e.g. a policy is still in development.

Information can be refused on the basis that it is not held by Inland Revenue if you have **no** grounds for believing that the information is either:

(i) held by another Minister or agency subject to the OIA or LGOIMA, or
(ii) connected more closely to a Minister or agency subject to the OIA or LGOIMA.

If Inland Revenue believes the information is held by a Minister or another agency, the request should be transferred to that Minister or agency. See *Transfers*.

Inland Revenue is only required to provide information that is **already held**, it is **not** required to create information in order to respond to a request. The information requested should be held at the time the request is received. See the section on whether information is held.

Maintenance of the law

Under section 6(c) of the OIA, information may be refused if releasing it would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detention of offences.

Inland Revenue has statutory enforcement abilities and the ability to prosecute. However, in terms of revenue information, it is unlikely that we would rely on this section. We would probably refuse the request on the basis that disclosure was contrary to s.18 of the TAA - disclosure would prejudice the maintenance of the law.

Section 6(c) may be relevant where the information is not revenue information, or the information is sensitive revenue information and there is a permitted disclosure.

Tax confidentiality and sensitive revenue information

When Inland Revenue receives an OIA or Privacy Act request, the first consideration is whether the information requested is sensitive revenue information and therefore confidential under the TAA. The requirements of the TAA take precedence over the OIA and PA.

Section 18(1) of the TAA requires all officers of Inland Revenue to keep confidential sensitive revenue information, unless the disclosure is permitted under sections 18D to 18J of the TAA. We are also not allowed to disclose revenue information if disclosing the information would adversely affect the integrity of the tax system or the maintenance of the law.

If the information is sensitive under section 18 of the TAA, we must usually refuse the request, or at least refuse that part of the request. See example wording here.

Step 1: Is the information revenue information?

First determine whether the information is revenue information. Revenue information is defined in section 16C (2) of the TAA as any information acquired, obtained, accessed, received by, disclosed to, or held by the Commissioner under or for the purposes of a revenue law; or under an information-sharing agreement.

Revenue law is defined in section 16C(1), and includes:

- the Inland Revenue Acts
- the Accident Compensation Act 2001, the Accident Insurance Act 1998, the Accident Rehabilitation and Compensation Insurance Act 1992, or the Accident Compensation Act 1982
- the New Zealand Superannuation Act 1974, and
- any Act that imposes taxes or duties payable to the Crown.

If the information is not held under or for the purpose of a revenue law, or under an information-sharing agreement, consider the information under the PA or under the OIA.

If the information is revenue information, determine if it is sensitive revenue information.

Information-sharing agreements

An information-sharing agreement includes an approved information-sharing agreement made under section 18E(2) of the TAA; an agreement made through consent under section 18E(3) of the TAA; agreements made by regulations under section 18F of the TAA for public services purposes.

Information-sharing agreements also include memoranda of understanding where Inland Revenue can share information with other agencies.

Step 2: Is the information sensitive revenue information?

Sensitive revenue information is defined in section 16C (3) of the TAA as revenue information that relates to the affairs of a person or entity and:

- identifies, or is reasonably capable of being used to identify, the person or entity, whether directly or indirectly, or
- might reasonably be regarded as private, commercially sensitive, or otherwise confidential, or
- the release of which could result in loss, harm, or prejudice to a person to whom or entity to which it relates.

Reasonably capable of identifying a person or entity

The information does not necessarily of itself need to disclose a person/entity's identity but could enable someone to identify a person/entity. For example, where the information disclosed could be combined with information that is publicly available to identify the person/entity, then it may be "reasonably capable" of identifying a person or entity.

Private, commercially sensitive, or otherwise confidential

Information "might reasonably be regarded" as private if it is reasonably foreseeable that information belonging to particular persons is of a type that the persons concerned would prefer is kept private. It is common practice to have confidentiality clauses in commercial contracts, particularly in a competitive industry. It is also reasonable to conclude that a company would want the fact that Inland Revenue is investigating them kept private, as this could damage their reputation.

Commercially sensitive

What is commercially sensitive is usually measured in terms of the possible business harm or negative commercial effect through the disclosure of that information. The release of information of a commercial nature relating to a taxpayer should be approached with caution even if the information is anonymised. For example, during a tax investigation, we may come across information about a product that is being developed and kept secret pending an application for a patent.

Otherwise confidential

This is a catch-all provision, although it is difficult to see what information would be confidential that is not already private or commercially sensitive. However, "otherwise confidential" would cover any information reasonably regarded by the taxpayer/s to whom it relates as confidential. To determine this, as well as considering the nature of the information, it is necessary to consider the basis on which it was provided. For example, if the person provided the information on the condition that it was kept confidential, then the information may be "otherwise confidential".

The release could result in loss, harm, or prejudice to a person to whom, or entity to which, it relates

As well as commercially sensitive information, this would also include all forms of potential damage or detriment to any person or entity to whom the information relates. It would include physical or non-physical harm, monetary and non-monetary loss, reputational harm, and any disadvantage resulting from being prejudiced.

Aggregate or statistical data is not sensitive revenue information

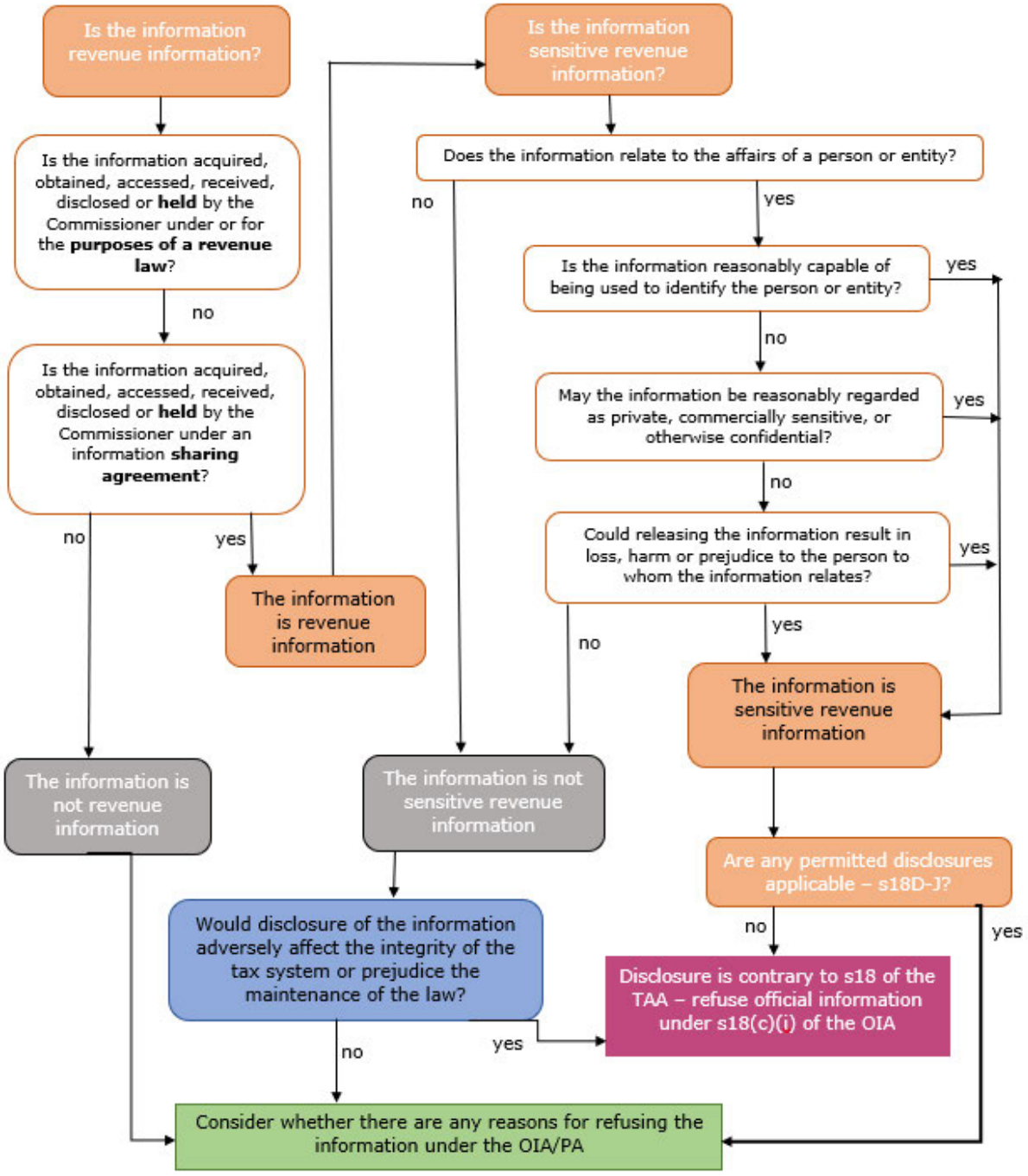
Aggregate data is a grouping of things that are not necessarily numbers focused.

Aggregate and statistical data is explicitly excluded from being sensitive revenue information, even if it contains information about a person or entity.

If the information is not sensitive revenue information, consider whether disclosure of that information would adversely affect the integrity of the tax system or the maintenance of the law. If it would not, the information should be considered under the PA or OIA (instead of TAA).

The following flowchart shows the steps to take to work out if information is revenue information or sensitive revenue information.

Revenue information or sensitive revenue information?



Integrity of the tax system and maintenance of the law

A request for revenue information should be refused if the disclosure of the information would adversely affect the integrity of the tax system or the maintenance of the law.

Before releasing revenue information that is not sensitive revenue information, consider whether communicating the information "would adversely affect" taxpayer perceptions that tax liabilities are determined fairly and impartially, that all taxpayers must comply with the law, and that Inland Revenue keeps individuals' and entities' tax affairs confidential.

When determining if disclosing the information would adversely affect the integrity of the tax system, ask yourself:

- What are the likely short and long-term effects on taxpayer compliance of releasing the information, and of not releasing the information?
- Could releasing the information assist Inland Revenue or taxpayers to make better decisions about how the current law applies, or assist in developing a better tax system?
- Could refusing the information cause taxpayers to view Inland Revenue as unnecessarily secretive and unwilling to promote greater taxpayer participation in the tax system?

Types of information that, if disclosed, may adversely affect the integrity of the tax system include:

- investigative techniques
- industry benchmarks
- audit strategy
- tolerance levels and thresholds, and
- new policy development.

If releasing the information is likely to have negative effects on compliance that outweigh any benefits to tax integrity from releasing it, the information should be refused under section 18(c)(i) of the OIA, as disclosure of the information is contrary to the TAA.

Contrary to legislation – section 18(c)(i)

Section s.18(c)(i) of the OIA allows information to be refused if to do so would be contrary to a statutory provision. This is the section to use when refusing information because disclosure is contrary to section 18 of the TAA.

Inland Revenue must not disclose sensitive revenue information unless there is a permitted disclosure. Refer to the *revenue information or sensitive revenue information?* flowchart to work out if the information is requested is sensitive revenue information and, if it is, whether there is a permitted disclosure.

If the information is revenue information:

- and disclosure would adversely affect the integrity of the tax system, or
- the maintenance of the law, or
- the information is sensitive revenue information

and there is no permitted disclosure under sections 18D to 18DJ of the TAA, the information should be refused under section 18(c)(i) of the OIA.

Maintenance of the law

The OIA and PA both have a ground for refusing information on the basis of "maintenance of the law". The Privacy Act allows agencies to collect, withhold, use or disclose personal information where it is necessary for the maintenance of the law. Under the OIA and PA, the maintenance of the law relates to law enforcement action by a public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences.

These reasons only require the maintenance of the law to be "prejudiced". This does not require the maintenance of the law to be negated or nullified. It would be enough if release could have a compromising or detrimental effect.

Example: Generic audit or investigative techniques

Information about generic audit or investigative techniques would be revenue information that is not sensitive revenue information because it is revenue information that applies generally and does not relate to a particular person. However, releasing this information is likely to have a material negative impact on taxpayer compliance because some taxpayers may attempt to use it to avoid their tax obligations.

This negative impact is likely to outweigh any benefits to the integrity of the tax system from releasing this information (from, for example, increased transparency). Therefore, information about generic audit or investigative techniques should not be released.

Another reason for not disclosing revenue information that is not sensitive revenue information is where the maintenance of the law would be prejudiced. This includes tax laws and laws administered or maintained by other agencies.

Example: Police investigation

An example would be where the Police have informed Inland Revenue that they are investigating a possible scam in a particular part of New Zealand. They have asked if Inland Revenue has any specialised investigative techniques that Inland Revenue uses in countering organised crime. The media has subsequently asked if Inland Revenue has been approached by the Police regarding any investigation into the suspected scam, and if so, where. This information should be refused if disclosure would prejudice the maintenance of the law by compromising the Police investigation.

Permitted disclosures of sensitive revenue information

Sensitive revenue information can only be disclosed if doing so is a "permitted disclosure" under sections 18D-J of the TAA.

Carrying into effect – s.18D(1)

Sensitive revenue information can be disclosed for the purpose of carrying into effect a revenue law, or for the purpose of performing or supporting a function lawfully conferred on the Commissioner under a revenue law.

Example

A customer has income tax arrears. You have issued a deduction notice, instructing the taxpayer's bank to deduct a sum of money. In this way, you have disclosed to the bank that the customer has tax arrears. This disclosure, however, is necessary for the purposes of carrying into effect the TAA.

Carrying out or supporting a function of the Commissioner – s.18D(2)

Sensitive revenue information can be disclosed under this section by a senior member of Inland Revenue with appropriate delegation, who has considered competing factors to reach a judgement that a disclosure is reasonable in the particular circumstances (guidance on the application of s.18D(2) can be found in Standard Practice Statement 11/07).

The first step is to assess if disclosure would be made in carrying out or supporting a function of the Commissioner. The functions of the Commissioner include:

- administering the tax system
- implementing the tax system, and
- improving, researching or reforming the tax system.

The second part of the test is to determine whether disclosure would be reasonable, after weighing and balancing the following five factors:

1. the Commissioner's obligation at all times to use best endeavours to protect the integrity of the tax system, and
2. the importance of promoting compliance by taxpayers, especially voluntary compliance, and
3. any personal or commercial impact of the communication or in any other way, and
4. the resources available to the Commissioner, and
5. the public availability of the information.

Disclosures to persons and their representatives – s.18G

Sensitive revenue information can be disclosed to the person (or their agent) in relation to whom the information is held. Clause 15 of schedule 7 of the TAA sets out caveats on provision of personal information. The Commissioner must consider whether:

- the information is readily available, and
- if it is "reasonable and practical" to provide the information.

If the information is not "readily retrievable":

- If the request is by or on behalf of an **entity**, the request may be refused under s.18(c)(i) of the OIA, as the information is sensitive revenue information and there is no permitted disclosure.
- If the request is by or on behalf of a **natural person**, the request may be refused under s.29(1)(i) of the PA, as the information is sensitive revenue information and there is no permitted disclosure.

If we consider that the disclosure of the information would adversely affect the integrity of the tax system

Although the information may be personal information, there would not be a permitted disclosure as it would not be "reasonable and practical" for the Commissioner to disclose the information.

Other permitted disclosures

Other permitted disclosures will not usually be relevant in the context of an OIA/PA request. If you need further advice, ask GES, subject matters experts, LTS, Corporate Legal, or Inland Revenue's Privacy Officer.

Security, defence or international relations of New Zealand

Under section 6(a) of the OIA, information may be withheld if disclosure would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand.

At Inland Revenue, this section may be relevant if we have concerns that the disclosure of the information may have an adverse effect on our relationship with a tax agency of another country. An example would be where we have concerns that a comment we have made in a briefing to a Minister, about another tax agency, would be likely to be interpreted in a negative way by the Government of that country.

As an agency, we do not comment on or hold views on the tax agencies of other countries.

Information entrusted by another country

Under section 6(b) of the OIA, information may be withheld if disclosure would be likely to prejudice the entrusting of information to the Government of New Zealand by another country or an international organisation.

At Inland Revenue, this section may be relevant where we have been provided information by another country's tax agency (perhaps under a mutual tax agreement) and we are concerned that, if the information is disclosed, this would be likely to adversely affect information being provided in the future.

Prejudice the safety of any person

Under section 6(d) of the OIA, information may be refused under this section if release would be likely to endanger the safety of a person.

The request is frivolous, vexatious or trivial

A request may be refused under section 18(h) of the OIA where the request is frivolous or vexatious, or the information is trivial. Please note that it is **the request** that must be vexatious, rather than the requestor.

The threshold for considering a request vexatious is very high. The Ombudsman's view is that requestors should not be unfairly denied the opportunity to make genuine requests. If you do use s.18(h), make sure to document your reasons thoroughly.

What makes a request frivolous, vexatious or trivial?

You can consider factors such as:

- The request would impose an unreasonable burden on the agency due to being very complex or for large amount of information.
- The request lacks any serious purpose or value (consider discussing the request with the requestor, as there may be a purpose that is not evident to the agency).
- The requestor has specifically stated that their intention is to cause disruption, irritation or distress to the agency, or there is evidence that suggests this.
- The request causes unreasonable harassment or distress to staff (seeks personal information about staff, makes derogatory comments about staff, or the burden of dealing with the request will necessarily fall to particular staff.
- The language or tone of the request is aggressive, offensive or abusive.

- There have been repeat requests for the same information (although there may be genuine reasons for a repeat request for exactly the same information).
- The requestor's conduct has raised safety concerns for staff.
- The information has already been provided by the agency.

Trivial information includes autoreplies, read receipts, meeting arrangements, emails noting that a document is attached, correspondence referral cover sheets, and information that contains only a fleeting reference to the subject of the request.

However, in requests for large amounts of information, extracting trivial information is unlikely to be worth the time and effort.

Alternatives to using the frivolous, vexatious or trivial grounds

If you prefer not to use section 18(h), you have three options:

Refuse under section 18(f): If the concern is the administrative burden, consider using s.18(f), substantial collation or research, and consider consulting with requestor to refine or consider charging.

Refuse under section 18(g) There is no obligation on an agency to create information in order to respond to a request. Where the request is in the form of questions, particularly argumentative or "loaded" questions, consider using s,18(g), the information is not held.

Refuse under section 9(2)(g)(ii) Where the concern is the protection of staff, consider using s.9(2)(g)(ii), withholding is necessary to maintain the effective conduct public affairs through the protection of staff members from improper pressure or harassment.

Examples of wording to use

Public interest

In refusing your request for information, I have taken into account the public good considerations in section 9 of the OIA.

Rights of review

If you're withholding any information, you must inform the requestor of their review rights. The wording we use is:

If you disagree with my decision on your OIA request, you can ask an Inland Revenue review officer to review my decision. To ask for an internal review, please email the Commissioner of Inland Revenue at: CommissionersCorrespondence@ird.govt.nz.

Alternatively, under section 28(3) of the OIA, you have the right to ask the Ombudsman to investigate my decision. You can contact the office of the Ombudsman by email at: info@ombudsman.parliament.nz.

Refusing revenue and sensitive revenue information (s.18 of the TAA):

Example of refusal wording - revenue information

The information you have requested is revenue information and I consider that disclosure of the information would adversely affect the integrity of the tax system/the maintenance of the law *[may wish to explain reasoning]*. I am therefore refusing your request under section 18(c)(i) of the OIA, as disclosure would be contrary to section 18 of the Tax Administration Act 1994 (TAA).

Example of refusal wording - sensitive revenue information

The information you have requested is sensitive revenue information. Inland Revenue is required to maintain confidentiality in respect of sensitive revenue information, and it is therefore necessary to refuse your request under section 18(c)(i) of the OIA, as disclosure would be contrary to section 18 of the Tax Administration Act 1994 (TAA).

Tānga o te whakautu ki te tono mō ngā Pārongo Ōkawa

Publication of responses to requests for Official Information

This paper outlines Inland Revenue's approach to the publication of responses to requests for Official Information

Introduction

One of the key principles of the Official Information Act 1982 (OIA) is to make information more freely available, which promotes good government, openness and transparency, and it fosters the public's trust and confidence in Inland Revenue.

Publishing OIA responses can make it easier for the public to obtain information they would otherwise seek through the OIA, which can reduce the administrative burden, and time delay, that OIA requests can place on Inland Revenue and requesters.

Application

While Inland Revenue supports proactive release (including publishing appropriate OIA responses) in line with the OIAs purpose, this approach does not direct business units to always proactively release (or publish) responses to requests for official information. It encourages consideration of whether information produced by Inland Revenue should be considered for release publicly, as part of business-as-usual activity where the content is in the public interest.

We will continue to ensure that our staff exercise caution and undertake necessary due diligence before making information publicly available. This includes consideration our confidentiality requirements set out in Section 18 of the Tax Administration Act 1994.

Definition of terms

Official information means any information that Inland Revenue or its employees[1] hold. It includes:

- documents, reports, memos, letters, texts, emails (including drafts).
- non-written information such as video or voice recordings.
- internal policies and guidelines.
- information that is known to Inland Revenue but has not yet been written down.

[1] Includes permanent or fixed-term staff, contractors and consultants

Publication of requests means making responses to requests under the OIA available to the public after it has been provided, where the information is of public interest. This includes:

- publishing Inland Revenue's documents (such as annual reports, statements of intent, research reports, briefing) on our website.
- publishing the same, or edited, information that we have already or are about to release to a requester under the OIA.

Public interest equates to the concept of public good, or legitimate public concern. It does not simply mean that information is 'interesting to the public'. Inland Revenue considers it is in the public interest to release information that:

- is useful or meaningful to the public.
- provides insight into the work we do.
- promotes the purposes of the OIA.

If our consideration of the public interest in disclosure outweighs the need to withhold the information, it should be released.

Key principles

Inland Revenue will:

- consider our confidentiality obligations under Section 18 of the Tax Administration Act 1994.
- observe the spirit of the OIA and comply with its requirements.
- as a primary consideration, release information unless there is 'good reason' to withhold it.
- consider whether the information is of public interest.
- consider whether releasing additional information would help to provide context or mitigate any harm from the information being released.
- where information is being released in response to an OIA request, consider whether the information is suitable to be published on our website.
- undertake due diligence and assess potential effects of releasing information (including the effects on personal privacy) before releasing official information.

Decision-making

Business groups producing official information should consider proactively releasing the information in situations where the information:

- tells the public about how we undertake our functions.
- is about our projects, corporate functions or advice to ministers.
- or the topic it covers, has been requested more than once.
- meets the 'public interest' test.
- if made publicly available, would not create any legal risk to Inland Revenue.

The following framework can be used as a basis to assist with decision-making

- **Information released by default (high public interest and low risk)**
  Information that is likely to be of high value to the public and there is little or no risk from releasing it.
- **Information released in a case-by-case basis (high public interest and higher risk)**
  Information that is likely to be of high value to the public, but the associated risks will require consideration before the information is published.

- **Not proactively released (low public interest and low risk)**
  The low public interest does not justify the administrative burden of publishing the information.
- **Not proactively released (low public interest and high risk)**
  The costs of managing the risks are outweighed by the limited value to the public.

The withholding grounds in the OIA need to be considered to ensure that proactively publishing information doesn't prejudice one of those interests.

Due Diligence

When the decision has been made to proactively release information, the relevant documents must undergo due diligence. There are four parts to this –

Review to assess liability

Section 48 of the OIA protects agencies from liability that may otherwise result from making information available in good faith under the OIA. These protections do not extend to proactive publication of information, even if the information has previously been released under the OIA.

Inland Revenue must therefore consider any potential liability, whether civil or criminal, that might result from the proactive publication of any official information.

The relevant documents need to be reviewed to establish their appropriateness for release – to ensure that the information will not expose Ministers or Inland Revenue to any civil or criminal liability (including defamation, copyright or breach of privacy).

Appendix A provides information on risks that Inland Revenue might need to consider before proactively releasing information.

Risk assessment and mitigation

The content must be assessed to identify any media, political and/or reputational risk; and establish how any risks can be mitigated.

Business groups must assess the risks of proactively releasing information, which involves assessing the potential effects of releasing the information in good faith – and considering if:

- the information includes any content that would be withheld if it was requested under the OIA or other legislation.
- any potential liability (civil or criminal) might result – as mentioned earlier.
- any of the information is subject to section 18 of the Tax Administration Act 1994.
- the public would need access to any other information to make sense of the information being considered for proactive release.

Advice should be sought from Governance and Ministerial Services or Corporate Legal if there is any doubt about whether releasing the information would pose a risk.

Consulting affected parties

Individuals and organisations outside of Inland Revenue (including other government agencies) need to have the opportunity to comment if we intend to release information about them, or provided by them, that is not already publicly available.

No surprises

The proactive release of information should not come as a surprise to the Commissioner, the Executive Leadership Team or relevant Minister(s). They need to be informed, in advance, if there

are any matters of significance in the documents that have been considered for release – particularly where these matters may be controversial or may become the subject of public debate.

Publication of responses to OIA requests

GMS will consider whether it is appropriate to publish responses to requests for official information, with recommendations made as part of the final approval process. Requests from customers about information relating to the tax affairs of specific entities will not be considered for publication. .

In responses to requests for official information, we will include a paragraph to say that the response to them, and the information provided, may be published on Inland Revenue's website. All personal information or information that may identify them will be redacted.

In some instances, information requests may be refused and no information is released (other than the reason for declining the request). For example, where the information is (or will soon be) publicly available under section 18d. These responses should still be considered for publication if there is public interest in that topic. Each case should be considered on a case-by-case basis.

Redactions

Content from information that we proactively release can be redacted. Redactions do not need to be identified with the related sections of the OIA.

Officials' personal information

Section 9 of the OIA allows the withholding of a person's name to protect their privacy. The Ombudsman's view is that it is not necessary to withhold the names of officials acting in an official capacity and names should, in principle, be made available when requested.

Inland Revenue's approach is to release the names of all Inland Revenue staff, unless there is a good reason to withhold it. We will withhold telephone numbers, email and signatures.

Responsibilities

The **business group creating** any official information is responsible for ensuring that they identify whether this should be considered for proactive release – this also includes assessing whether a response to an OIA request should be considered for publication.

Governance and Ministerial Services (GMS) is responsible for overseeing the proactive release process and can provide guidance on assessing any risks (including political) that may arise from proactively releasing information. GMS will keep a record of information that has been proactively released. GMS will also be responsible for uploading information to Inland Revenue's website.

Corporate Legal is responsible for helping business groups identify and assess any legal risks that may arise from proactively releasing information.

The **business groups' Service Leader** is responsible for approving the information to be proactively released, with input from GMS.

Marketing & Communications is responsible for helping identify any publicity risks that may arise from proactively releasing information.

Other business groups (including Finance Services and Policy & Regulatory Stewardship) can provide advice on any sensitivities associated with information that a business group is considering for proactive release.

Further information

For further information, this paper should be read in conjunction with other guidance material on responding to requests for official information. You can find this on the **Governance, Ministerial and Executive Services** Intranet page.

Other references:

- Section 18 of the Tax Administration Act 1994
- Ombudsman's guide on 'public interest'
- Official Information Act 2020
- Privacy Act 2020

Appendix A

This table provides information on some of the risks that Inland Revenue might need to consider before proactively releasing information.

Key question	What to consider
Is there a contractual interest in the information proposed for release?	Consider whether we need to redact information to protect contractual obligations or whether the information should be released at all.
Is any of the information we are proposing to release subject to copyright?	Consider if the information is the creative work of others, their trademarks or certain confidential business information. If so, the information's owner must give us permission to publish it.
Does the information proposed for release say or do something that could harm the reputation of another person, group or organisation?	Ensure that we understand and assess any defamation risks that could arise from releasing the information. Seek **Corporate Legal** advice if necessary.
Does the material contain any information that must be withheld under the terms of any other legislation?	Take other legislation (for example Section 18 of the Tax Administration Act) into account if the information proposed to be released contains contents hat must be withheld under the terms of that legislation. Seek **Corporate Legal** advice if necessary.

What is the Official Information Act 1982 (OIA)?

The OIA is a law that applies to ministers and central government agencies, enabling people to request official information. Inland Revenue (IR) is a government department, so all information we hold is subject to the OIA.

The purpose of the OIA is to make information available to the people of Aotearoa New Zealand so that they can effectively participate in the making and administration of the Government's laws and policies. The OIA also ensures government ministers and agencies are held accountable for their decisions and actions.

All information that IR holds is official information. This doesn't just mean information in documents – it includes things like sound recordings, film, emails, text messages, Microsoft Teams chats, and information known to IR employees that isn't recorded in writing.

OIA requests can be made in any form, including verbally, and they don't have to mention the Act. The person making the request doesn't have to tell us why they want the information or what they'll do with it. Anyone physically present in New Zealand is eligible to make an OIA request, as well as New Zealand citizens, permanent residents and companies that have a place of business in New Zealand.

Providing and withholding requested information

Under the OIA, we must provide official information when it is requested, unless there are good or conclusive reasons not to.

The OIA sets out the reasons for which official information can be withheld. For example, we can withhold information to protect people's privacy or the maintenance of the law. This means we wouldn't release information about a specific customer to another person, and we wouldn't release information about the tax system if someone could use that information to get away with tax avoidance or evasion.

Section 18 of the Tax Administration Act 1994 (the TAA) requires us to keep all sensitive revenue information confidential and sets out the circumstances in which sensitive revenue information can be disclosed. The requirements under the TAA take precedence over the OIA.

The OIA doesn't cover information that an individual requests about themselves. This is covered by the Privacy Act 2020, which aims to promote and protect individual privacy.

Which Act applies? Some student loan-related examples

Taika asks for information about his own student loan. The law that applies to this request is the **Privacy Act**. There's unlikely to be any problem with supplying this information. All frontline IR people can respond to Privacy Act requests (apart from those involving child support, which are handled by a specialist team).

Nikau asks for information about their sister's student loan. But Nikau is not an authorised person on their sister's account. The laws that apply to this request are the **TAA** and the **OIA**. We wouldn't supply this information.

Gina asks for data about how many student loan borrowers there are and how much they owe on average. The laws that apply to this request are the **TAA** and **OIA**. No one's privacy is impacted, as no information about specific people can be inferred. We would likely provide this information.

Alex asks for information on overseas-based borrowers' student loan repayment obligations. There would be no need to treat this as an OIA request, as general

information about obligations is easily found on our website. We can just refer Alex to where she can find the information she needs.

Tim asks for information about the number of student loan borrowers who are currently being monitored by IR because we're considering stopping them from leaving the country. The laws that apply to this request are the **TAA** and the **OIA**. We wouldn't supply this information, as it could be used to help people get around their compliance obligations.

How quickly do we need to respond to an OIA request?

By law, we must respond to an OIA request with our decision on the request within **20 working days**. The Ombudsman's website has a calculator to work out the due date for the response. The clock starts when IR receives the request, not when it is picked up to be completed.

This means we must send any OIA request to the right person as soon as we can. This will be the team or person with the knowledge and experience to apply the relevant laws, provide the requested information and consider any other important factors.

If you don't know who should respond to an OIA request, check with your team leader or manager, or with Governance and Ministerial Services (GMS) at oia@ird.govt.nz.

Can we extend the deadline for responding?

The OIA allows us to extend the 20-working-day timeframe if the request is for a lot of information, or we would need to search through a lot of information and meeting the original time would unreasonably interfere with IR's operations.

The OIA also lets us extend if we are unable to reasonably respond within 20 working days because we need to consult another agency, organisation or person on the request.

We must let the requestor know in writing that we're extending the deadline, and we must do this within the original 20-working-day deadline.

What is GMS's role in OIA requests?

OIA requests come from many different people for many different reasons. The requested information is often on political topics and can end up in the public eye.

IR's Governance and Ministerial Services Team (GMS) can provide guidance on the OIA and help with managing OIA requests.

GMS also coordinates and helps with OIA requests where there might be some risk associated with releasing the information. GMS ensures that these requests are carefully managed and that the necessary stakeholders are engaged at the right time.

Get in touch with GMS as soon as possible if the request:

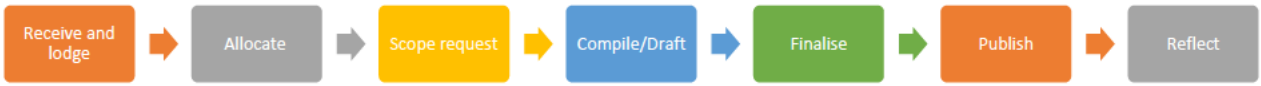
- comes from the media, a Member of Parliament, or a political party's parliamentary research unit
- relates to an issue that has received recent media coverage
- contains any issue involving alleged misconduct, mistakes, or serious oversight by IR people
- relates to information that the Minister may be asked about
- could potentially affect IR's relationship with important stakeholders.

If you have any questions about responding to OIA requests, please contact the team at oia@ird.govt.nz.

GMS – OIA Process

Managing an OIA request

This document outlines the process and practise for managing an OIA request.



Receive and lodge	
Process	'Business Support' enters the case into the Tool (see separate instructions on how to do this) and actions any Non-OIA cases.

Allocate	
Process	• 'Level 2' allocates case to a team member for action. • Provide relevant notes in the comments field, including which L2 is allocated to support on this OIA. • Check the **Minister report required** box (if required).

Scoping/planning This action should be done within the first few days of receiving a request	
Process	• Move case to **IN PROGRESS** in the Tool. • Create any relevant Tasks in the Tool. • If appropriate, select the **02 Consider for Publication** tag. • If required, set up a scoping meeting. • Save any scoping/decision notes into the Tool.
Practice	• Review the request to ensure you understand the request and that the scope of the request is clear. • Search system for similar requests for the same information (including previously published responses[1]). • Inform the business Units/SME of the request and if needed, hold a scoping/planning meeting – consider who else needs to be involved or made aware of this request. • Decide who is responsible for what – gathering and reviewing material, drafting the response and signing the response out. • Is 20 days enough time for the request – do we need to consider extending the request?

[1] You can also find these by filtering by the **03-OIA published** tag

Compile/Draft	
Process	• Keep in regular contact with those involved in preparing/compiling content. • Save a 'clean' copy of all documents that are in scope into STAX (this ensures that if an internal review is required at a later date, all information is accessible. • Save DRAFT response and 'Marked up' version of documents to be released into STAX. • If required, prepare the OIA coversheet for the Minister's office.

Practice	• Draft response to requestor
	  ○ If the decision is to **release information**, consider providing contextual information to assist with interpretation of the material being released (particularly for statistics or data).
	  ○ If the decision is to **withhold information**, ensure appropriate reasons are included in the response letter and in notes in the Tool (this ensures information is available if an internal review is required at a later date).
	• Ensure that the response notes whether any attachments to documents in scope, are included or not in the information released.
	• Although we are not the decision-makers, we need to read all the material that is considered part of the request and consider whether any reasons for redacting are in line with the OIA and our guidance.

Finalise	
Process	• Undertake any necessary consultation. • Response is reviewed by a Level 2 team member. • Arrange for sign-off by the appropriate person. • If the response is a ministerial OIA then material should be sent to the Minister's office for release. • If the response is an IR OIA then the response should be sent to the requestor (via the OIA tool where possible) • Ensure all related documents are saved into STAX (unredacted, marked up and redacted versions of information being released).

Publication of response	

Process	• Throughout the process, consider whether the response will be published after the response has been released (consult with business representatives if required).
	• In the Tool select the appropriate tag
	  ○ **02-Consider for publication** or
	  ○ **04-Not for publication**
	
	If the response will be published, save a redacted version (removing all personal information) into the Tool and name it '*22OIAxxxx Response for publication'.*
	
	These responses will be picked up by the Business Support and published on the website on a monthly basis.

Reflect	
Process	• Consider what went well, and why. • Consider what didn't go so well, and why. • Reflect on what you would do differently in the future for a similar case. • Share knowledge/learnings with the team.

Day-by-day OIA process

BS = Business Support, DS = Domain Specialist, L2 = Level 2 Domain Specialist

The below timeline is a guide. We aim to provide information to requestors as soon as available, therefore in many instances, the full 20 days is not required.

Out of Scope

Day 1

Request received through OIA inbox:

- L2 checks to see whether it is an OIA, and applies tags on how and who to action
- BS actions most tags and adds as much detail as possible to OIA tool
- BS scans (if required) and uploads request to Stax
- BS considers acknowledgment and uploads to Stax

Request received through OIA form (via website):

- OIA inbox receives alert from the OIA Tool notifying that there is a new OIA
- L2 check OIA tool regularly

- L2 reviews, adds further details to the OIA tool and allocates to team member
- L2 will set date if a copy is to be sent to the MoR's office either in advance of, or at the same time as, sending the response to the requestor. For an IR OIA, the time period will be dependent on if there is requirement to consult with the Office, or solely to inform. For a MoR OIA, the time period is at the MoR Office's discretion, and is typically 3working days before release, this is done on a case-by-case basis

Consult – **5 working days** before OIA due date. This would generally be where there is shared content with the Minister's office and can be open for their feedback.

Inform (FYI) – 2 working days before OIA due date. This would generally be when it is IR content, but the MoR's office should be made aware in line with the no surprises convention. Same day: morning of for noting not for changes. Especially for media or MP OIAs.

Day 2 – or as soon as allocated

- DS reviews and checks the due date/s and determines due date for the business to supply the information (at least 5 working days before due date to allow for reviews)
- Adds subject, summary and tags to OIA Tool
- DS considers:
  - Previous similar OIA requests (or those published on the website)
  - Do we need a scoping/planning meeting? Who needs to attend?

- Consider risk (media, political, reputational). Notify appropriate manager, media and GMS Domain Lead (if required)
- Any clarification needed? (Clarification within 7 working days resets the day count)
- Consultation with other agencies?
- Potential transfer? (Within 10 working days of the request)
- Necessary for legal involvement. If required Conrad is key contact, second contact is <insert> Give legal a heads-up that a review of the OIA will be required on x-ish date.
- Necessary for media input?

- DS liaises with those in the Business Unit allocated to collate the information. Follows up with email and noting in the Tool. If a CCS data request, then cc Sandra and Estelle
- DS organises scoping/planning meeting, if required. Refer to stakeholder internal contact list.

Day 3/4 – Scoping/planning meeting (if required)

- Facilitated by GMS.
- Discuss any issues – possible extension? Potential transfer? Consultation?
- Confirm who will be responsible for the response. Who will be the contact point for GMS?
- Discuss timeframes (including time for next meeting with docs/response)
- Sign off process (Leader who owns the data will sign out)
- Is there a requirement for media lines and report to the Minister?
- DS follows up with an email to attendees with what was agreed to at the meeting, including action points and who these were assigned to.
- DS updates OIA tool with key deadlines, interpretation of the request, decision making considerations, who action points assigned to.
- Updates OIA tool with latest update on the OIA

Day 4-8

- Collation of documents by business/person responsible for the response.
- DS checks in with the contact person regularly.
  - Updates OIA tool with latest update on the OIA

Days 8–12

- DS required to:
  - review documents & reconsider whether Legal advice required
  - discuss any proposed redactions with Business Unit and mark these up
  - draft response
  - seek legal advice/manager support if necessary.

Out of Scope

Days 12-15

- Finalising the response and reviewed by L2
- Getting necessary sign offs
- Send to media to check if any media lines are required
- Decision on if response will be published
- Updates OIA tool with latest update on the OIA

Days 15-20

- If needed, send a copy of the response to the Minister of Revenue (MOR)'s office. 5 days prior to release if to be consulted on. 2 days prior to release if the office requires an FYI. Send to the MOR's private secretary (Helen Kuy) and cc:
    - the MOR's revenue advisor (Jason Batchelor)
    - the Associate MOR's advisor (Harper B)
    - the Commissioner's strategic advisor (Tania Sellers)
    - the Commissioner's executive support team lead (Jo Petrie) and
    - Ministerial Services (us).
- The private secretary roles in the offices of the Minister of Revenue and the Parliamentary Under-Secretary for Revenue are secondments from IR, but their email address is "@parliament.govt.nz" (not "@ird").
- The email should be classified "In confidence – internal, NZ Govt".
- There's an example of the email to send on the next page. The email should summarise the response and provide any background info. If we're refusing any info, we should explain why.
- Advisor File away the email into '01 OIA correspondence' in Ministerial Services inbox.
- For IR OIAs, the Minister's office will either provide a response to request for consultation or will note the response. For MoR OIAs, the MoR's Office will release these.

By day 20

- DS to finalise letter and documents
    - Naming convention: "24OIAXXXX signed response [LAST NAME]"
- DS updates tool, spreadsheet and STAX.
- Response sent by DS from OIA tool or by media (if response is to a journalist).
- DS collates emails and documents regarding OIA and files them in STAX.
- Redacted copy to be published is saved in STAX and the OIA tool, if applicable.
    - Proactive release of responses to OIA requests - Sept 2021.docx
    - Out of Scope

Further considerations

Out of Scope

Out of Scope

Out of Scope

Release of staff names in responses to OIA requests

This paper outlines Inland Revenue's approach to the releasing the names of Inland Revenue staff in response to information requests (including Privacy Act requests)

Introduction

The basic premise of the Official Information Act (OIA) is that information must be released on request unless there is a 'good reason' not to. In essence, it is where release would harm one (or more) of a series of protected interests. There are also some administrative reasons for refusing information requests.

The Ombudsman's general view is that staff names should, in principle, be made available. Such information normally only discloses an individual's employment and what they are doing in that role. Anonymity may be justified if a real likelihood of harm can be identified.

The Privacy Commissioner, in response to consultation by the Ombudsman, also considers there is a low level of privacy interest in the names of staff, and they should be released for reasons of accountability.

Inland Revenue's approach

Inland Revenue's practice has previously been to withhold the names and email addresses of staff below manager level.

This approach has now been updated and Inland Revenue will now release the names of staff where their names fall within the scope of the request for information, unless there are situations where staff have concerns about safety, improper pressure or harassment. Telephone numbers, email addresses and signatures will continue to be withheld.

These decisions should be considered on a case-by-case basis in the context of each request for information. If there is reason to believe that harm could result from the release of a staff member's name, they should be informed before the information is released. Any decision to withhold the names of any officials should be clearly justified and documented.

This approach applies to all requests for information.

Further information

Further information can be found in the Ombudsman Guide *Names and contact details of public sector employees (April 2020)*. If you have any further questions or concerns about this approach, please contact Governance and Ministerial Services (GMS) at oia@ird.govt.nz.

Out of Scope

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Managing Personally Identifiable Information (PII)

1 What is this Guideline about?

Privacy can mean different things to different people. Our focus here is about personally identifiable information (PII) collected for IR work activities, stored anywhere by IR employees. The guide explains the need to be aware and careful about how we create, collect, and store personal information and how to protect and manage it.

Collecting information about individuals is part of Inland Revenue's day-to-day activities in administering the tax system. NZ Legislation gives IR authority to collect personal information. We apply rigorous processes to govern how we obtain and manage this type of information to ensure the NZ public trust IR and to protect their right to privacy. We need to apply the same principles to all PII at IR.

This guideline covers all IR functions and activities and applies to all IR employees, contractors, and consultants. It can cover information about employees; names, titles, contact details, personnel information, as well as information we might obtain from external people, for events, meetings, and recruitment.

1.1 What business or technical need does this support?

Out of Scope

Out of Scope

Out of Scope

Out of Scope

Out of Scope

Out of Scope

2 Guide to Managing PII

2.1 What is Personally Identifiable Information (PII)?

PII is information about an identifiable individual or information where an individual can be identified. It is any information about a person and the information does not have to include their name.

Some examples are:

- health information,
- financial information
- personnel file,
- resume, or CV.

PII is any information that can be used on its own or with other information to identify, contact or locate a living person.

PII must tell the reader or hearer something about a person. If no one can be identified by the information, then it is not personal information. PII can be created in formal and informal business activities.

2.2 Where does PII come from?

PII gets created in many formal business activities: core activities such as tax and social policy administration, recruitment, performance appraisal, health & safety procedures, for example.

Informal business activities such as team building, meetings and collaboration activities may also contain personal information.

PII may be stored in a variety of forms, such as; on paper, electronic documents, content in Team sites, chat or email, data extracted from systems or in a person's memory.

2.3 What are the consequences of not managing PII?

People need to have trust and confidence that Inland Revenue will protect their information. It is mandatory to give IR information – people often don't have a choice - so we are held to a high standard when it comes to keeping PII safe and using it appropriately.

If IR doesn't handle PII properly there is a risk of information being used or disclosed when it shouldn't be. This may result in harm to affected individuals or IR's reputation and effect people's compliance with their tax obligations.

Manage your information

Managing information is the first step in protecting people's privacy.

Managing information means:

- understanding what purpose we collect information for and what it will be used for
- ensuring information is accurate, up-to-date, and fit for purpose
- complying with regulations and privacy requirements
- regularly disposing of information that is not required to be kept

Always pay attention to the storage, security, preservation, and disposal of information you create and use. Think carefully about where to store it, who is able to see it and how long you need to keep it for.

Unmanaged information poses a heightened risk that a privacy breach will occur. If no one takes care how PII is treated, then it may be found and used for a purpose other than the reason it was collected. It may be disclosed when it should not be or retained well after it should be. Information becomes out of date and unreliable the longer it is kept.

Risk of Privacy Breach

The ever-increasing occurrence of information breaches involving PII has contributed to an increased risk of identity theft for the individual whose sensitive data was exposed. Fines for data breaches can be considerable. In New Zealand the average amount awarded by the courts for a privacy breach is $10,000 and the highest awarded $168,000.

Sending or emailing information to the wrong people is the most common type of privacy breach at IR. When you create documents that include personal information you should double-check that the right "access permissions" are assigned to the document. This ensures that only appropriate people can access the information and if sending information by any means check you are using the correct address.

Spreadsheets can pose a risk because of all the information they can contain. If you must share information in a spreadsheet, protect the document with a password and if personal information does not need to be included then remove it.

Information breaches are harmful to individuals and organisations:

- **Risks to individuals**: identity theft, financial loss, significant emotional stress, blackmail
- **Risks to organisations**: loss of public trust, legal liability, fines, and remediation costs

Tips for preventing data breaches can be found on the Privacy Commissioner's website.

2.4 Why must we manage PII?

The Privacy Act

The Privacy Act requires everyone, including IR employees, to take reasonable measures to ensure appropriate security of all personal information, not just taxpayer information.

When in doubt consult our IR privacy officer for advice.

The Privacy Commissioner's Quick Tour of Privacy Principles outlines our obligations for managing PII.

In summary they are:

- You can only collect personal information if it is for a lawful purpose and the information is necessary for that purpose. You should generally collect personal information directly from the person it is about.
- Take reasonable steps to make sure that the person knows the purpose of collection, what it will be used for and who will receive it.
- You may only collect personal information in ways that are lawful
- You must make sure that there are reasonable security safeguards in place to prevent loss, misuse, or inappropriate disclosure of personal information
- People have the right to request access to, and correction of, their information
- Before using information ensure that it is accurate, complete, relevant, up-to-date, and not misleading
- Use and disclose information only for the reason it was collected unless an exception applies. (For exceptions to this principle under Government Information Sharing Agreements contact Corporate Legal)
- Do not keep information for longer than is necessary
- You may only disclose personal information in limited circumstances
- An agency may only disclose personal information to an agency overseas if the information will be adequately protected.
- You can only assign a unique identifier to individuals where it is necessary for operational functions. Generally, you may not assign the same identifier as used by another organisation

Approved Information Sharing Agreements

"Information Sharing" is the disclosure of information about an identifiable individual by a government agency to another agency, usually for a reason unrelated to the reason it was originally collected. An Information Sharing Agreement authorises agreed departures from some of the privacy principles when there is a clear public policy justification and its agreed, managed and formally documented.
Consult the Information Sharing Team

2.5 How do I manage PII?

- Apply the **privacy principles** to any PII you create and/or use
- **Minimise the collection**, use and retention of PII
- **Use secure links rather that attachments** to send PII. Copies of information sent to you as an attachment copy should not be stored long term as this creates duplication
- **Evaluate the material** and assign correct security classification, access and disposal of PII-Out of Scope
- **Keep your own personal information about yourself private**, e.g. reference material, personal notes, your own CV in the appropriate IR Content system- OneDrive.

2.6 Common Examples of PII

Examples of PII include, but are not limited to:

- **Name**: full name, maiden name, or alias
- **Unique Identifiers**: passport number, driver's license number, taxpayer identification number, financial account numbers, bank account number or credit card number
- **Contact information:** home address, work address or email address, telephone numbers
- **Personal characteristics:** photographic image (especially face or other identifying characteristics), fingerprints, retina scan, voice print, or other physical or behavioural descriptions that can be used to identify a person
- **Linked or linkable information:** information that is linked or linkable to one of the above categories like date of birth, place of birth, race, religion, I.P. address, social media content, political views, weight, activities, employment information, medical information, education information, financial information or any other unique identifiers.

3 Responsibilities

The following establishes the broad accountabilities and responsibilities of the key internal stakeholders applicable to this Guideline

3.1 Who does what?

Who	What
Leaders of functions, groups and teams	Must: • support and communicate the Guideline to their employees, contractors and consultants to ensure they understand the Guideline • demonstrate compliance with the Guideline.
All employees, contractors and consultants	Everyone who needs to make use of this Guideline for work purposes must ensure that they understand and comply with this Guideline.

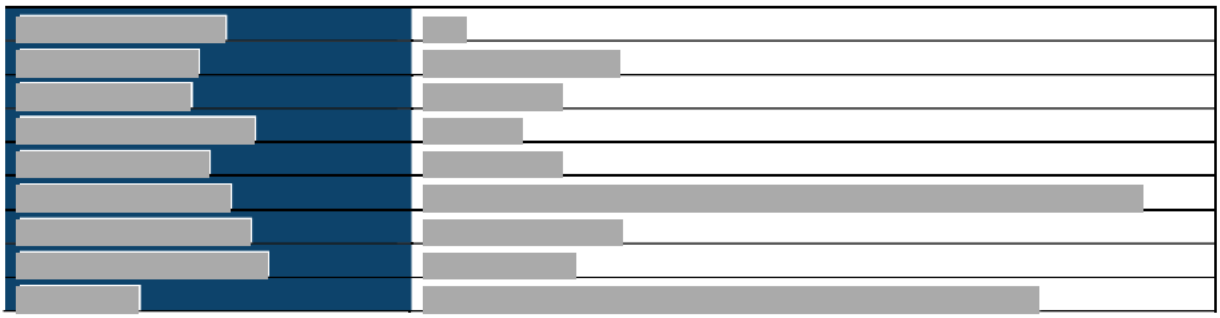
4 Terms and Definitions

Term	Definition	Source
Approved Information Sharing Agreement (AISA)	Formal agreement authorising disclosure of information about an identifiable individual by a government agency to another agency	
Personally Identifiable Information (PII)	Information about an identifiable individual or information where an individual is capable of being identified	
Content Developer	A person responsible for developing the content of this Guideline, under instruction from the Document Owner.	
Document Owner	A person with authority to approve this Guideline on behalf of the Functional Owner.	

5 Where to find out more

This Guideline is available to all employees, contractors and consultants. The current version of this Guideline is stored in the Governance Centre. If you require any further information, please contact the Document Owner or Content Developer (refer Section 5.1).

Out of Scope



OIA requests

The information on this page will help you to recognise and respond to requests for official information. It explains the three Acts that set out how IR must deal with these requests.

What is the Official Information Act 1982 (OIA)?

The OIA is a law that applies to ministers and central government agencies, enabling people to request official information. Inland Revenue (IR) is a government department, so all information we hold is subject to the OIA.

The purpose of the OIA is to make information available to the people of Aotearoa New Zealand so that they can effectively participate in the making and administration of the Government's laws and policies. The OIA also ensures government ministers and agencies are held accountable for their decisions and actions.

What is official information?

All information that IR holds is official information. This doesn't just mean information in documents – it includes things like sound recordings, film, emails, text messages, Microsoft Teams chats, and information known to IR employees that isn't recorded in writing.

How do people make OIA requests?

OIA requests can be made in any form, including verbally, and they don't have to mention the Act. The person making the request doesn't have to tell us why they want the information or what they'll do with it. Anyone physically present in New Zealand is eligible to make an OIA request, as well as New Zealand citizens, permanent residents and companies that have a place of business in New Zealand.

Providing and withholding requested information

Under the OIA, we must provide official information when it is requested, unless there are good or conclusive reasons not to.

The OIA sets out the reasons for which official information can be withheld. For example, we can withhold information to protect people's privacy or the maintenance of the law. This means we wouldn't release information about a specific customer to another person, and we wouldn't release information about the tax system if someone could use that information to get away with tax avoidance or evasion.

Section 18 of the Tax Administration Act 1994 (the TAA) requires us to keep all sensitive revenue information confidential and sets out the circumstances in which sensitive revenue information can be disclosed. The requirements under the TAA take precedence over the OIA.

The OIA doesn't cover information that an individual requests about themselves. This is covered by the Privacy Act 2020, which aims to promote and protect individual privacy.

> Which Act applies? Some student loan examples
>
> Taika asks for information about his own student loan. The law that applies to this request is the Privacy Act. There's unlikely to be any problem with supplying this information. All frontline IR people can respond to Privacy Act requests (apart from those involving child support, which are handled by a specialist team).
>
> Nikau asks for information about their sister's student loan. But Nikau is not an authorised person on their sister's account. The laws that apply to this request are the TAA and the OIA. We wouldn't supply this information.
>
> Gina asks for data about how many student loan borrowers there are and how much they owe on average. The laws that apply to this request are the TAA and

OIA. No one's privacy is impacted, as no information about specific people can be inferred. We would likely provide this information.

Alex asks for information on overseas-based borrowers' student loan repayment obligations. There would be no need to treat this as an OIA request, as general information about obligations is easily found on our website. We can just refer Alex to where she can find the information she needs.

Tim asks for information about the number of student loan borrowers who are currently being monitored by IR because we're considering stopping them from leaving the country. The laws that apply to this request are the TAA and the OIA. We wouldn't supply this information, as it could be used to help people get around their compliance obligations.

How quickly do we need to respond to an OIA request?

By law, we must respond to an OIA request with our decision on the request within 20 working days. The Ombudsman's website has a calculator to work out the due date for the response. The clock starts when IR receives the request, not when it is picked up to be completed.

This means we must send any OIA request to the right person as soon as we can. This will be the team or person with the knowledge and experience to apply the relevant laws, provide the requested information and consider any other important factors.

If you don't know who should respond to an OIA request, check with your team leader or manager, or with Governance and Ministerial Services (GMS) at oia@ird.govt.nz.

Can we extend the deadline for responding?

The OIA allows us to extend the 20-working-day timeframe if the request is for a lot of information, or we would need to search through a lot of information and meeting the original time would unreasonably interfere with IR's operations.

The OIA also lets us extend if we are unable to reasonably respond within 20 working days because we need to consult another agency, organisation or person on the request.

We must let the requestor know in writing that we're extending the deadline, and we must do this within the original 20-working-day deadline.

What is GMS's role in OIA requests?

OIA requests come from many different people for many different reasons. The requested information is often on political topics and can end up in the public eye.

IR's Governance and Ministerial Services Team (GMS) can provide guidance on the OIA and help with managing OIA requests.

GMS also coordinates and helps with OIA requests where there might be some risk associated with releasing the information. GMS ensures that these requests are carefully managed and that the necessary stakeholders are engaged at the right time.

Get in touch with GMS as soon as possible if the request:

- comes from the media, a Member of Parliament, or a political party's parliamentary research unit
- relates to an issue that has received recent media coverage
- contains any issue involving alleged misconduct, mistakes, or serious oversight by IR people
- relates to information that the Minister may be asked about
- could potentially affect IR's relationship with important stakeholders

Resources

Here are some resources to help you in responding to OIA requests.

Information relating to privacy requests can be found on the Privacy intranet site.

s52(3)(b)(i) of the OIA & s18(3) of the TAA

Out of Scope

- Out of Scope
- Out of Scope
- Out of Scope
- Out of Scope

Tools

- IR's Guide to OIA and Privacy Act Requests
- OIA training: Full guide
- OIA training summary
- Out of Scope
- IR's approach to publication of responses to requests for official information (proactive release)
- IR's approach to releasing names of IR staff in response to information requests

Contact us

If you have any questions about responding to OIA requests, please contact us at oia@ird.govt.nz.

Privacy

Dawn Swan is Inland Revenue's Privacy Officer. Dawn oversees Inland Revenue's privacy compliance and practice and helps create and manage IR's privacy programme.

Privacy officer

The Privacy Officer identifies privacy obligations and mitigates privacy risk to IR and taxpayers arising from day-to-day business and changing business practices, the data environment and customer expectations.

- Day-to-day, we safeguard taxpayers' personal information to maintain trust and confidence.
- The information/data handling environment changes as data holding is decentralised. Transformation processes bring increased risk of privacy breaches, both unintended (eg: software glitches) and cultural (eg: 'everything is open now').
- Customers want increased convenience (eg: no returns to file) but will react to any inconvenience by going directly to social media. The increased volume of personal data needed to provide this convenience 'raise the stakes' for potential privacy complaints.

In an agile, improving organisation, privacy must be included in all steps of the operation including planned changed. Privacy by Design is current best practice and the privacy sector's equivalent of agile development.

Our Privacy Officer

The Privacy Officer is responsible for:

- Encouraging compliance with the Privacy Act.
- Providing advice on privacy issues, impact assessments, incidents, breaches, and complaint handling.
- Assisting the business as required to ensure privacy controls are baked in to processes and systems, address privacy issues or possible breaches of privacy
- Ensuring that privacy information, guidance and training is available to staff.
- Monitoring policies to check compliance and ensuring there are procedural safeguards.
- Representing IR's privacy interests with external parties and liaising with the Office of the Privacy Commissioner and the Government Chief Privacy Officer.
- Reporting on privacy-related issues.

Mission Statement

The Privacy Officer identifies privacy obligations and mitigates privacy risk to IR and taxpayers arising from day-to-day business and changing business practices, the data environment and customer expectations.

- **Day-to-day:** We safeguard taxpayers' personal information to maintain trust and confidence.
- **Changing data environment:** The information/data handling environment is changing as data holding is decentralised. Transformation processes bring increased risk of privacy breaches, both unintended (eg software glitches) and cultural (eg 'everything is open now').
- **Changing customer expectations:** Customers want increased convenience (eg, no returns to file) but will react to any inconvenience by going directly to (social) media. The increased volume of personal data needed to provide this convenience 'raise the stakes' for potential privacy complaints.

Privacy affects all areas of Inland Revenue. It can't be managed by one person. A number of people within Inland Revenue also have important operational roles in terms of privacy compliance:

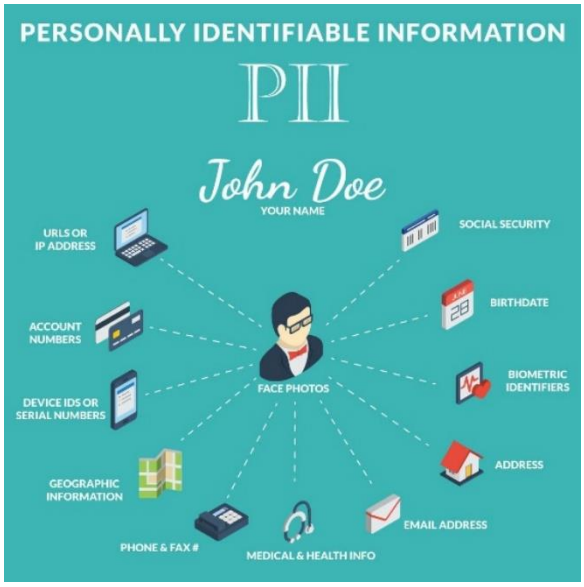
- Day-to-day operations require employees to deal with personal information as part of their duties.
- An incident management team respond to breaches.
- Complaints Management respond to privacy complaints raised by customers and Government and Executive Services respond to Privacy Act complaints notified by the Privacy Commissioner.

It's important that everyone takes an interest in privacy and understands just how important it is. Feel free to contact Dawn if you have any questions or ideas about what you'd like to see on this site.

What is Privacy?

Privacy can mean different things to different people but the Privacy Act is all about personal information and how it's managed.

Personal information is defined as information about an identifiable person, so the information must tell the reader or listener something about a particular person. If no one is identified by the information then it is not personal information.



Information about organisations (ie. companies or trusts) is not personal information. Inland Revenue holds and uses a lot of personal information so we must keep that information safe and only use it for specific purposes.

The Privacy Act 2020 sets out 13 principles that govern how all agencies have to treat personal information and gives individuals some control over who has their information.

It's important that Inland Revenue treats personal information correctly and we all have a role to play in that.

We live in an information age where personal details are very valuable. Sometimes you want to share your details to get a benefit (deals and discounts), for convenience (doing business online), or to connect with others. Every time you give someone your details, you also expect them to be kept safe.

What happens if your personal information is misused or not kept safe? You don't trust the agency that didn't do enough to protect you. You might get spammed, be contacted or harassed by strangers, feel unsafe, or have your identity stolen. In extreme cases,

when an address is disclosed when it shouldn't have been, some people have to relocate to feel safe again.

That's why privacy is so important. People should know who has their personal information and what it will be used for.

Agencies should be open with people about what they will do with personal information that it holds. Privacy is about trust and transparency.

Privacy at work

Protecting the integrity of the tax system is the responsibility of all Inland Revenue employees. The public expect us to be beyond reproach in our behaviour and delivery of work and to keep their information secure.

The following are some tips to help you ensure that you are doing everything possible to comply with IR policies and minimise the risk of privacy breaches.

Tips for all staff

- Before hitting 'Send' on an email, double check you are sending it to the right person (do not rely on the auto-populate feature in Outlook).
- Don't leave printed documents at the printer, make sure you take them with you.
- Before sending letters or emails to a customer, double check that no other customer's details are included.
- Do not email work to your personal email address.
- Do not take customer information home with you unless this is absolutely necessary. Keep it secure at home.
- Place any paper rubbish that contains personal information in the document destruction bins or use a shredder to destroy it.
- Ensure that your desk is clear of work at the end of the day.
- Lock your screen every time you step away from your device.

Tips for frontline staff

- Follow the correct validation process in START Help.
- Try not to have more than one customer account open at a time. This ensures that you're looking at one customer's details and minimises the risk of giving them someone else's information or entering a note under the wrong IRD number.
- Be careful when copying and pasting IRD numbers from screen to screen. Check the IRD number is for the right customer.
- Be careful when using the suspend screen option and ensure that you have the correct customers details on the screen in front of you.
- Ensure that you enter the correct person's details under the correct IRD number.
- Have one letter or application on your desk at one time. File the others in an in-tray or folder and only get them out as you work on them.

The Privacy Act

The Privacy Act 2020 governs how individuals, organisations and businesses collect, use, disclose, store and give access to personal information. Personal information is defined as information about an identifiable, living person. If information does not identify anyone, the Privacy Act will not apply.

The Privacy Act applies to 'agencies'.

Almost every business, organisation, and individual that handles personal information is considered an agency under the Privacy Act – whether they are a government department, private company, religious group, school, or even an individual person in some cases. The Act also applies to organisations that 'carry on business' in New Zealand even if they don't have a physical presence here.

At the heart of the Privacy Act are 13 privacy principles that state how agencies must treat personal information. These principles reflect internationally accepted standards for good personal information handling:

1. Only collect necessary personal information for a lawful purpose.
2. Get information direct from the person concerned unless an exception applies.
3. Tell people what you're going to do with their information.
4. Don't collect information by means that are unfair or intrusive.
5. Once you hold personal information, keep it secure.
6. People are allowed to request, and have access to, their own information.
7. People can ask for their information to be corrected.
8. Information should be accurate before it is used.
9. Don't keep information for longer than is necessary.
10. You can't use personal information collected for one purpose for another unless an exception applies.
11. You shouldn't disclose personal information unless an exception applies.
12. You can only disclose personal information overseas if the recipient country has comparable privacy protections.
13. Don't assign unique identifiers, or require someone to disclose one, unless it's lawful.

The Act also sets out specific reasons when an agency may refuse to release personal information to a requester, rules around information sharing, information matching, and public registers.

Privacy at IR

It is vital that IR builds and maintains the trust and confidence of individuals who provide us with their personal information. Protecting this information is a core responsibility of everyone at IR and is endorsed in our Code of Conduct.

The Tax Administration Act provides that we all must keep information confidential and privacy is wider than confidentiality.

The Privacy Act 2020 sets out obligations covering the collection, storage, use and disclosure of personal information and each business area in IR is responsible for meeting these obligations. Every employee and contractor needs to understand and apply the basic requirements necessary to meet IR's privacy obligations.

The Privacy Act also governs information sharing arrangements between agencies. IR is involved in many important information matching and sharing agreements and you can find out more about these, and how information sharing works, on the Information Sharing site.

IR's Privacy Policy explains what IR's obligations are and what we must all do to manage privacy. Please take the time to read the Privacy Policy and get to know your privacy obligations.

There is a specific Staff Personal Information Policy which explains IR's commitment and practices in relation to ensuring the privacy of staff personal information.

Information security standards and processes include the Acceptable Use Standard, Access Controls, Information Handling, Password & Authentication Standard, Internet and Email Use.

IR has an Information and Knowledge Management strategy, policies and principles, including guidance on retaining and deleting information.

People Policies & Guidelines on People & Culture's site covers:

- Use of business tools.
- Disclosure & conflict of interest.

- Confidentiality & secrecy.

Governance

Mary Craig, Deputy Commissioner Enterprise Design & Integrity (ED&I), has overall responsibility with the Executive Leadership Team for privacy.

IR's Privacy Officer is Dawn Swan who reports directly to Mary. Dawn provides advice and assistance on privacy matters and the privacy programme. The programme consists of policies and processes across IR, training and education, breach and incident management and risk identification and controls.

The Privacy Officer also manages IR's relationship with the Office of the Privacy Commissioner and the Government Chief Privacy Officer (GCPO). IR's Privacy Officer should be advised if the Privacy Commissioner or GCPO becomes involved in any matter you are dealing with.

At IR, we have a decentralised privacy office governance structure. One Privacy Officer oversees privacy compliance, practices and advises, while decision-making for day-to-day activities is delegated. This allows decisions and information to flow bottom-to-top and widens the span of control.

Privacy breaches

While we must do all we can to ensure a privacy breach doesn't occur, where one does happen, it's important that it is managed properly and dealt with immediately. Proper breach management is vital to ensure IR retains the trust of the individual whose information has been breached and enables them to protect themselves.

All privacy incidents and breaches are managed by Complaints Management, part of PD&D (Planning, Design & Delivery).

Privacy incidents or breaches should be reported immediately through the **Sensitive Incident notification form (this form is used for reporting privacy breaches or lost/stolen devices)**.

Contact the Privacy Officer for more advice or if you're not sure whether to report an incident.

Training

A **Privacy Awareness e-learning module** is available through Atea.

Privacy is also covered in the following e-learning modules:

- **Our Code of Conduct – Tikanga Whanonga:** (MANDATORY) This provides a walk-through of the four sections of our Code and has a number of interactive scenarios for you to consider along the way.
- **Keeping Information Safe at IR :** (MANDATORY) Gain a better understanding of our policies and procedures that help us keep information safe, learn about some key threats, how our behaviours can make a significant difference in protecting IR's, and our own, personal information.
- **Navigating IR - Information Handling & Security:** required learning for all staff new to IR. Focuses on security at IR, the Code of Conduct, information classification and handling and keeping our information safe.
- **Integrity discussion topics** - these are scenarios to work through as a team and include topics such as Inappropriate Conversations, Accidental email breach, After work drinks and Unauthorised access to START. Use them to start a conversation.

If you have specific training requirements, or want privacy training, contact the Privacy Officer.

Managing People's Personal Information

At IR we deal with a lot of people's personal information, so it's really important that we all know how this information should be treated – whether you should or shouldn't be able to see it, who you can share it with and how you can protect it properly.

Handling people's personal information

We hold lots of personal data for all NZ citizens and have a number of powerful technology tools. So, it's important we all ensure that no matter which system we use, we are always protecting people's information – both for our customers and us as IR staff.

In order to do this, you need a basic understanding on what 'personal information' is and how you can identify it as well as the impact of how you are sharing this information.

Different information categories

There are a few different ways we talk about personal information here at IR. For a start there's customer's personal information, but we also hold a lot of personal information about us, the staff, as well.

Here we will try to break it down for you:

Information held by the Commissioner is divided into three categories:

- **Revenue information** ("RI" or "Revenue Information");
- **Sensitive revenue information** ("SRI" or "Sensitive Revenue Information");
- Other information.

Revenue information (RI)

Revenue information relates to information held by Inland Revenue. RI is all the information that we acquire and hold in relation to our role in administering Revenue Law and Social Policy.

Revenue Information could include, for example:

- thresholds and tolerance levels;
- profiling information;
- investigative techniques;
- operational policies and procedures;
- aggregated compliance statistics; and
- programme evaluations.

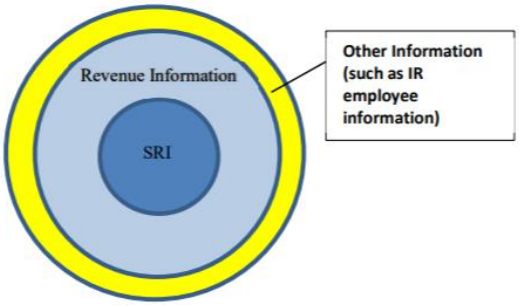
Sensitive revenue information (SRI)

Sensitive Revenue Information is a subset of Revenue Information.

It means: Revenue Information that identifies, or is reasonably capable of identifying our customers, (directly or indirectly) or that might reasonably be regarded as private or commercially sensitive, or the release of which could result in loss, harm or prejudice to the person it relates to.

Other Information

Other information not falling into the definition of Revenue Information (or SRI) includes information held by Inland Revenue for purposes outside of its statutory revenue and social policy roles, such as personal information about employees (e.g. home phone numbers), or held for other corporate reasons such as commercial agreements or leases Inland Revenue is a party to.



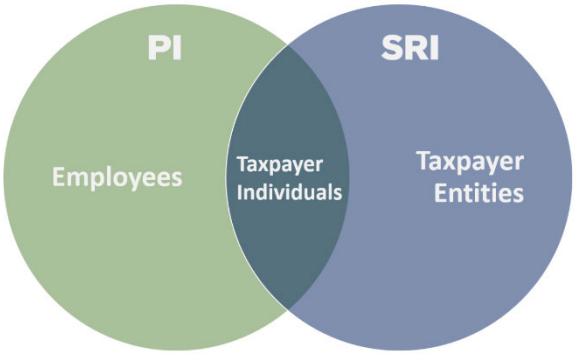
Personal Information (PI)

PI is any information about a living, identifiable person. Anything you can look at and say, "This is about a specific person". PI is intended to protect personal privacy. The SRI category is intended to protect the integrity of the tax system. It just happens to be that a lot of SRI is PI.

Personally identifiable information (PII)

PII refers to any data that can be used to identify a specific individual by using Personal information (PI). This can include information such as a person's name, address, IRD number, date of birth, and other sensitive information. It can be any information about a person, the content does not have to include their name.

Most of what we do at IR uses people's personal information – from dealing with customers, registering them for voice ID to managing your team's leave or updating your details in Ātea. We wouldn't get much done if we didn't use people's information.



Key tips for handling people's personal information

To do our job well, we need to be trusted custodians of information. So here are some things to think about:

- Access and use people's personal information **only when you have a valid business reason to do so.**
- If you're not sure, ask yourself: Is there a relevant business purpose for accessing or sharing this info?
- Don't look at any customers information just because you're interested. Only look at information that is required for you to do your work, don't browse as you can get into very serious trouble if you do!
- It's okay to discuss someone's circumstances (taxpayer or IR staff) for valid work reasons but think about whether you need to identify them and where you do this

- Do keep people's personal information secure – store it appropriately and restrict access if necessary
- Don’t collect personal information from customers or staff unless you actually need it
- Do think about how you want your own information to be treated and offer the same respect to customers and staff.

Privacy breaches

It's important that everyone takes an interest in privacy and understands just how important it is. Privacy can mean different things to different people but the Privacy Act is all about personal information and how it’s managed. Protecting the integrity of the tax system is the responsibility of all Inland Revenue employees. The public expect us to be beyond reproach in our behaviour and delivery of work and to keep their information secure.

For any questions regarding Privacy in IR you can contact Dawn Swan IR's Privacy officer - s9(2)(a)

How can a Privacy breach happen in IR?

Despite our best efforts to keep information safe, sometimes we fail. So here’s some examples of where things can go wrong and what we can learn.

Privacy breaches happen when personal information is compromised, usually by being disclosed when it shouldn't have been. Don’t forget that a privacy breach with customer information is also likely to be a breach of confidentiality (under the Tax Administration Act).

Unsurprisingly, many breaches happen in CCS as it deals directly with customers, but no business area is exempt! Anyone who deals with PII of customers, staff or colleagues, can cause a breach.

Here are some examples on how these mistakes can be made

Mistake 1 – Disclosing by email

Many of IR’s privacy breaches happen when we send an email or web message to the wrong person. For example, if:

- an email about a staff members performance issues are sent to their whole team instead of the person concerned,
- we incorrectly send another government agency a staff members salary information,
- we disclose details of a customers student loan debt to a relative.

These sorts of breaches are made even worse if we incorrectly attach information to the email, like:

- an Excel spreadsheet containing customer names, IRD numbers and enquiries for IR to action
- pre-filled forms, debt relief applications, student loan statements, Child Support admin review documents, unsuccessful job application letters.

Mistake 2 – Verbal disclosures

When we are speaking to customers, we need to take care that we don’t talk about other people's affairs. Don’t disclose information (unless they are a Nominated person) like:

- an individual's income details to their spouses,
- a company director’s personal debt when talking to an agent about the company,
- that a relative has applied for child support,
- the name of a receiving carer who has asked their name to be withheld

But don't think this is just a CCS issue – Everyone has to be careful - if you're talking about anything work related, be aware of your surroundings.

Mistake 3 – not keeping information safe

Do not:

- leave documents containing personal or revenue information on the printer, or abandoned outside IR like at a café,
- leave an IR device behind such as on a train, plane, bus or at a venue,
- take USB devices containing IR information outside of IR unless absolutely necessary (and if you do, keep them secure),
- also definitely don't use real customer information in presentations or training.

For guidance on responding to a privacy breach or for more information, refer to privacy beaches.

So, what can we learn from these mistakes?

To ensure we don't make these sorts of mistakes listed above, here are some practical tips for you to follow.

- Always check you are sending an email to the right recipient – it only a takes a few seconds to look at whose name is in the "To" box
- If you're sending an email to a lot of people, especially outside of IR, use the "BCC" function so email addresses can't be seen by all recipients
- Check you've attached the correct document to an email (or letter if you're putting it in the post)
- If sending documents internally send a link instead of a copy
- Don't leave personal information lying around so others can see it
- Lock your device when not using it – this applies in the office and when working from home (WFH)
- If taking information out of the office first ask if you really need to and, if you do, always secure it in a bag or compendium
- Watch what you say and where you say it especially if you can be overheard
- When WFH, don't let others see your work, store hard copy documents appropriately
- If you use START, ensure you add information to the correct customer record.

Resources

To find out more about what has been covered, here are some further resources to assist you.

Personally Identifiable Information Guideline
Privacy at IR
Corporate Legal - Information Law at IR
Privacy breaches

Remember, if you don't know or if you're in doubt – Find out! You can email Dawn Swan - IRs Privacy officer or for any IKM questions email us at AskIKM@ird.govt.nz

Tips to keep your information safe

On this page we share tips on how to keep your own personal information safe.

Social media

- Only be Facebook friends with people that you actually know.
- Be cautious when accepting invitations on LinkedIn from people you don't know.
- Don't post your address, phone number or credit card details online.

- Check privacy settings on your social media accounts regularly.
- Don’t post holiday snaps while you’re on holiday (people will know exactly where you are and that you’re not at home). Post them when you get home.
- Similarly, don’t give out your exact location at exact times on social media unless you want everyone to know where you are.
- Take care when uploading photos to the internet. Location data is often added to images via a phone's camera or an app, so details of where a photo has been taken within eight metres can be uncovered.
- Be careful who you trust with your information and details - they could post it online.
- If you want to post information on your page about others’ travel plans, check with them first – they may not want your friends to know their itinerary.
- When installing a new app, read the permissions. Many apps want to access your contacts, email address, and browser history and will pass this onto third parties. If you’re not comfortable giving them this information, don’t install the app.

Online security

- Consider use your middle name as your 'online only' surname. Any websites which are truly secure, and legally require your real name (banks etc) will then address you using your real surname. Any site which only knows your 'online' surname will only ever use that name.
- Similarly, use a nickname for your online presence.
- Change passwords regularly and don’t use the same one twice.
- Have a separate, low-limit credit card to limit your risk when buying online.
- Have more than one email address – one for registrations on sites, another for a particular group of friends and/or another for family.
- Make regular back-ups, use anti-viral and anti-phishing software.
- Don't use public WiFi to check online banking.
- Keep a close eye on credit card statements and reconcile any transactions. Contact your bank immediately if there’s a transaction you didn’t make.
- Don’t click on links in emails from someone you don't know, and if someone you know sends you something odd, check with them before opening it.
- When an online site has mandatory fields that are not relevant to the transaction, fill them with trivia such as the CEOs name or their own 0800 number or email address.
- Consider your online information to be like any piece of personal property - you can control what happens to it to some extent - but it will never be fully protected.
- Use a Virtual Private Network (VPN) when doing "sensitive" stuff on your mobile or laptop.
- Treat any information that you put online to be public information. You have very little control over who will copy and disseminate it and you can’t protect your information when someone else decides to make it public.

Other tips

- Ask to have your personal details suppressed from public registers such as your council’s Rating Roll. If you have concerns about your safety, you can also register for the Unpublished Electoral Roll rather than have your details publicly available.
- Shred airline boarding passes with Q codes - they give access to personal data plus past and future travel.
- When retailers ask for your personal details when making a purchase ask them why they need the information. Don’t be pressured into providing the information if you don’t want to. Any genuine business will respect your wishes.
- Read the fine print before agreeing to sign up to anything – especially the privacy statement. This should tell you what your information will be used for and who it may be passed onto

- To protect yourself from identity theft, securely dispose of mail that contains personal information, like bills or bank statements, and never put documents that contain personal details in the recycling bin.
- If you don't want to receive unsolicited marketing calls to your home telephone number, or unsolicited marketing mail to your home, you can add yourself to the Do Not Call and Do Not Mail registers operated by the Marketing Association.
- If someone asks to take a copy of driver's licence, ask them why this is necessary. The licence contains a unique identifier (the licence number) and the Privacy Act states that you are not required to disclose this information to anyone but NZTA or Police. If they need the licence to verify your identity, they can view it, so it's not necessary for them to copy the unique identifier and other information. Black out your personal details and the licence number.
- Ask providers to remove all your personal information when you close accounts, cancel subscriptions, or leave loyalty programmes.

Privacy Act requests

Under the Privacy Act individuals are entitled to request and have access to their personal information. They can also ask for their information to be corrected.

Principle 6 of the Privacy Act gives people the right to request access to information about themselves. **Principle 7** gives people the right to request that their information be corrected.

The Act covers private and public sector agencies and even groups like clubs. This means you have the right to see what information is held about you by most organisations (although the media and courts are exempt).

Inland Revenue is subject to the Privacy Act. However, there is also a requirement under section 18 of the Tax Administration Act (TAA) that all officers must keep confidential sensitive revenue information unless the disclosure is a permitted under the TAA. When responding to a Privacy Act request, you will also need to consider this section. Generally, information about a customer, that has been provided to Inland Revenue by that customer, can be released to them.

General points

- Personal information' is defined as information about an identifiable individual - so it must tell the reader or listener something about a specific person. If someone is not identified by the information they won't be entitled to it under the Privacy Act;
- We must respond to an information request within 20 working days. The law says during that time we should decide whether to grant the request and let the requester know of that decision. The information requested doesn't have to be provided within 20 working days but it's best practice to release information as soon as possible - if you can release it within 20 working days, do;
- A request doesn't have to be in writing and it can be made verbally;
- People are only entitled to information that is readily retrievable;
- Requesters are not entitled to original documents;
- The agency receiving the request should make information available in the way preferred by the individual requesting it (for instance hard copy, or electronic or if they want to view the information, you should make arrangements to make this happen);
- A public sector agency cannot charge for making information available under the Privacy Act.

Privacy vs the OIA and TAA

What's the difference between a Privacy Act and Official Information Act request?

The Official Information Act (OIA) gives people the right to ask for access to any information held by a public sector agency.

The Privacy Act gives people the right to ask for access to their own information held by any agency.

So if you want information about yourself it's a Privacy Act request, if you want any other information including information about other people (and it's held by a public sector agency) it's an OIA request.

Here's more info about OIA requests.

Example 1: if a child support customer (let's say the father of a child) wants a copy of information IR holds about them this would be a request under the Privacy Act. However, if the father also wanted information about the mother of the child, this would be an Official Information Act request as that information is not about them.

Example 2: IR receives a request from Jo Bloggs for a copy of our Corporate Security policy. This is an Official Information Act request as the information is not about Jo Bloggs (so it's not his personal information) but it is information held by IR.

What about section 18 of the Tax Administration Act?

Section 18 of the Tax Administration Act (TAA) imposes a duty on revenue officers to maintain the confidentiality of sensitive revenue information and not disclose it unless the disclosure is a permitted disclosure that meets the requirements of sections 18D to 18J or Schedule 7. It also prevents disclosure of other revenue information where that would adversely affect the integrity of the tax system or prejudice the maintenance of the law.

Sensitive revenue information means:

- information held by the Commissioner in connection with a revenue law (and for a purpose in s16B(1)
- that identifies, or is reasonably capable of being used to identify, a person or entity, whether directly or indirectly; or
- that might reasonably be regarded as private, commercially sensitive or otherwise confidential or
- the release of which could result in loss, harm, or prejudice to a person to whom, or an entity to which, it relates.

When the confidentiality requirement in section 18 of the TAA is applicable (ie the information requested is sensitive revenue information), it is necessary to consider whether the information should be made available under the permitted disclosures to section 18. For example, we can disclose sensitive revenue information to the person to whom the information relates or their representative under Part B, Schedule 7 of the TAA.

Occasionally we receive requests from customers who **want to know who has accessed their information and why**. They may ask for a copy of the **access log** that shows who has accessed their information in START. The view of IR's technical specialists is that an access log is not automatically made available to customers. See further information on the page about reasons to refuse requests.

Process when responding to a request

How will I know it's a Privacy Act request?

The requester will be asking for a copy of their own information such as their own student loan statements, child support letters or maybe a complaint they've sent in. The information will identify them personally in some way.

The requester could also be a lawyer or tax agent acting for someone else. If it's a parent or nominated person, check that they are correctly authorised to act on the other person's behalf.

Requests could come in by letter, email, fax or over the phone (they do not have to be in writing).

What if I'm not sure?

Contact the requester to clarify what they're asking for. You might even be able to give them the information over the phone.

Who should respond?

Responsibility for a request should be allocated to the actual person who is going to collate and draft the response. Ideally this will be someone who understands the part of the business the customer has been involved in. For instance, if it's a child support customer, then someone within child support, who understands the information held, should be assigned responsibility.

How much time do I have to respond?

You have to respond as soon as reasonably practicable but no later than **20 working days** after the day on which the request is received. During this time, you must make a decision on the request and let the requester know. Usually the information to be disclosed will be provided at the time the decision is conveyed to the requester. Inland Revenue can be prosecuted if it doesn't respond within 20 working days.

The definition of 'working day' does not include most Public Holidays. The Privacy Commissioner has a 20 working day calculator on the front page of its website to help you figure out when you need to respond.

It's good practice to establish a timeline for responding. Work backwards from the 20 wording day due date and leaving a buffer of at least 2 days in case there are delays. But remember, while the time limit is 20 working days, **your obligation is to respond as soon as reasonably practicable.**

What if I need more time?

If you won't be able to make a decision within 20 working days, you can extend the time to respond but only if:

- The request is for a large quantity of information, or meeting the request will necessitate a search through a large quantity of information; or
- Consultations necessary to make a decision on the request are such that a proper response to the request cannot be made within the original time limit.

You cannot extend the time for any other reason.

You extend the time limit by writing to the requester, letting them know why you can't meet the 20 working day limit and letting them know what the new timeframe will be.

Out of Scope

What do I need to do?

Step one

Collate the documents or information being asked for.

The Automation Team have developed a tool to assist the staff who process Privacy Act requests. The Note Extractor efficiently summarises all (or some) correspondence notes from a customer’s account, with the choice of exporting as a Word document. This eliminates the need for staff to manually go through a customer’s account and copy and paste screens.

Have a good look at the request and read it carefully - is it for specific documents or more general? If it's for specific documents, locate those documents. If the request is general, check what databases or information you're able to access and see if you can locate information about the requester that falls within the scope of the request. You must make a reasonable search for information that falls within the scope of a request.

Look in relevant physical and electronic locations. Don't hesitate to get specialist help from records or IT staff.

If a requester has a myIR account, you could also advise them they can access some information through that and we don't have to provide copies. You could also phone the requester and ask them what they want, this can save time and effort in the long run.

Identify and consult with key staff who are likely to know what information exists and where it might be held.

If the request is from an IR employee or contractor, this should be referred to People and Culture.

Step two

Analyse the documents and see if there is any information that should be withheld from the requester. For instance, is the information about someone else? Is there a current investigation that might be affected if the information was released now? Reasons you can refuse to provide information can be found here.

Consult with others as necessary. The privacy officer is happy to provide advice on when the Privacy Act withholding grounds can apply.

TIP: Keep a record of any information that is withheld from a requester and why. When preparing documents that will have information blacked out, make three copies of each document: a clean copy, a mark-up copy (that shows what parts of the document will be withheld and why), and a redaction copy (when the information has been blacked out). The redacted copy will be sent to the requester.

If the requester makes a complaint to the Privacy Commissioner's office, we will have to provide a copy of our response including what information we refused to provide.

Step three

Draft a response using a template letter. Have it peer reviewed by a manager, Legal Services or Corporate Legal, especially if we are refusing to provide information, and then send it.

Requests to correct information

Under principle 7 of the Privacy Act, individuals have the right to ask that their information be corrected. However, the information does not have to be corrected.

If you receive a request for correction, decide if the information should actually be corrected. For instance if someone's date of birth or address is wrong then we would certainly want to update that information and would agree to correct it.

However, if someone disagrees with a decision made by IR and wants that corrected, we do not have to make any changes.

Principle 7 states that if an agency is not willing to correct information, it should attach a statement of correction to the information at issue. Usually, the statement is provided by the individual themselves and records the correction sought. The statement should then be attached to the information in such a way that they will always be read together. Let the requester know that their statement has been attached and give them a copy.

If IR attaches a statement of correction it should, if reasonably practicable, inform anyone to whom the information has been disclosed that a statement of correction has been added.

Reasons to refuse a request

The right to have access to personal information under the Privacy Act is not absolute and sections 49-53 of the Act provide some reasons why information may be withheld. This page provides the most common reasons why information may be withheld.

When providing screen-shots to requesters, Inland Revenue used to redact the user ID, screen system ID and screen identifier. However, in May 2015, the Chief Information Security Officer rated the security risk of releasing this information as *Low*. Given the effort involved in redacting (removing) this on every screen, it was recommended this information didn't have to be deleted when releasing screen-shots to requesters.

Maintaining the law

Disclosure of the information would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial - section 53(c).

Agencies that have criminal law enforcement functions (including Inland Revenue) can rely on this section. It's important that agencies that maintain the law can investigate and prevent crime and other offences. Sometimes, there's a real risk that releasing information to a requester could get in the way of investigating and detecting offences.

Agencies should release as much information as they can without prejudicing their ability to maintain the law. For example, releasing a summary of information can be a good way to give a requester as much information as possible, while not revealing investigation techniques.

This section can also be used to withhold the names of informants.

Example:

Donald Duck runs a distribution company. Mickey Mouse has contacted IR and said that Donald is not declaring all of the goods that he sells, and is paying his nephews, Huey, Dewey and Louie, in cash so they aren't paying tax. IR's investigation team starts to look into Donald's business. Donald finds out and asks IR for a copy of its investigation file so he can see what's been uncovered. IR can refuse to provide Donald with its file as disclosing some of the information at this stage may prejudice the investigation. If Donald finds out the details of what's being investigated, he could hide evidence or influence witnesses.

Breach of another's privacy

Disclosure of the information would involve the unwarranted disclosure of the affairs of another individual - section 53(b)

This section is designed to protect the privacy of people other than the requester. A requester's right of access to information about themselves is very strong but sometimes other people's privacy rights are even more important. This section is most often used where information about the requester is also information about someone else (for instance, information about family members).

Disclosing information about the other person must be 'unwarranted' and disclose the 'affairs' of another person. 'Affairs' has been interpreted broadly and applies to private situations as well as aspects of ordinary life pursuits or professional business. Even someone's name will constitute their 'affairs'.

In deciding whether disclosure is 'unwarranted,' you have to balance the requester's right to access information against the other person's privacy rights. Consider:

- What does the information reveal about the other person?
- Is the information confidential or sensitive?

- What were the other person's expectations about how the information would be used and disclosed? Were they told it would be treated confidentially?
- What harm might there be to the other person if the requester gets the information - for instance, would they be harassed, would it result in serious damage to relationships or affect their business standing?
- If the requester already knows the information about the other person, releasing it is unlikely to be unwarranted.

Example:

In the example above, Mickey has made a complaint to IR about Donald Duck. Donald asks IR for a copy of the complaint that was made about him. IR could withhold Mickey's name under this section of the Privacy Act, as releasing his identity would be an unwarranted disclosure of his affairs. Mickey thought he was being a good citizen by letting IR know about Donald's alleged illegal practice and expected his name to be kept confidential. If IR told Donald who the complainant was then this would prejudice the future supply of such information. IR relies on the free flow of information from third parties in order to detect and prevent offences. If the identities of informants are released, those people would not provide information, which would prevent offending from being discovered.

In this case, IR could release general details to Donald of what the allegation is without disclosing who the informant was.

Another law prohibits the information being released (TAA's section 18)

Another law prohibits or restricts information from being released - section 24(1)(b)

The Privacy Act can be overidden by other laws that authorise, require, prohibit or restrict the availability of information. For example, section 62 of the Insolvency Act 2006 provides there must be a public register of people who are discharged or undischarged bankrupts. Because this is required under the Insolvency Act a person cannot make a Privacy Act complaint about their name being made public.

Section 18 of the Tax Administration Act is an example of a law that prohibits or restricts information being made available, unless communicating the information is to carry into effect tax law or an exception applies. If you're refusing a request using section 18, this will override the Privacy Act reasons to withhold so use the following text:

Information is refused under section 24(1)(b) of the Privacy Act 2020 as disclosure is prohibited under another Act, namely section 18 of the Tax Administration Act 1994 (officers to maintain confidentiality). Disclosure of the information requested does not fall within any of the specific permitted disclosures to confidentiality, or would adversely affect the integrity of the tax system or would prejudice the maintenance of the law under section 18(3).

Request to know names of staff who have accessed someone's information

Occasionally, we receive requests from customers who want to know who has accessed or read their information and why. They may ask for a copy of the **access log** that shows who has accessed their information in START.

The view of IR's technical specialists is that an access log is not automatically made available to customers. We do not withhold the names of staff that appear in START notes (see IR's approach to the release of staff names in response to an OIA request) but an access log is a tool that sits behind START.

Often customers ask for the access log as they are concerned an IR employee may have accessed their information without proper authority. If this is the case, refer the

customer to Integrity Assurance (Out of Scope) in the first instance. The Integrity team can investigate the concerns if the customer provides the name of the employee they suspect is involved and why they believe their file may have been accessed.

After that investigation is complete, we can then consider if providing the access log, or part of it, is appropriate. The **access log** is considered revenue information so we need to consider the test in section 18 of the Tax Administration Act in deciding whether to release it (section 18 overrides the reasons in the Privacy Act for withholding information). If the release of the access log would adversely affect the integrity of the tax system or would prejudice the maintenance of the law then we may withhold it.

A danger to safety or risk of harassment

Disclosure would endanger the safety of any individual - section 49(1)(a)

Disclosure would create a significant likelihood of serious harassment of an individual - section 49(1)(b)

Sometimes releasing information to a requester may put someone's physical safety at risk: either the requester him or herself, an employee of the agency, or someone else. However. there must be some evidence to indicate that a danger in fact exists. If there is evidence that physical harm will result if the information is released, the agency can withhold the information.

If there is a risk releasing information would result in someone being seriously harassed then the information can also be withheld. Safety is more important than rights of access to information.

Evaluative material

The information is evaluative material and disclosure of the information, or of information identifying the person who supplied it, would breach a promise made to that person that the information, or their identity, would be held in confidence - section 50

Evaluative material is very specific and only applies to evaluative or opinion material compiled solely to determine someone’s suitability, eligibility or qualifications for employment, appointment, promotion or removal from employment (for instance, a reference check).

Evaluative material is information about what someone thinks about the person who's asking for the information - it's a judgment about the person's skills, their character, or their qualities.

The agency must be able to show that the person who gave them the evaluative material (the supplier) did so on a clear understanding that the material was to be kept confidential or that they wouldn't be identified as the source of the material. For instance, there is a record on file. If there's no record, to claim confidentiality it has to be obvious from the circumstances that the supplier *must* have expected that it would be kept confidential. Would the supplier have given the agency the evaluative material if he or she thought the agency would hand it over to the person concerned? If the answer is no, then it's confidential.

Legal professional privilege

Disclosure of the information would breach legal professional privilege - section 53(d)

When people go to see a lawyer, they need to know that what they say, and the lawyer's advice, will be kept confidential. There are two types of privilege:

1. 'Solicitor/client privilege' protects information contained in communications between a lawyer and their client undertaken for the purpose of seeking or giving advice, and the communications were intended to be confidential;

2. 'Litigation privilege' protects communications between a lawyer and their client or third parties relating to court proceedings. The document(s) requested must have come into existence when litigation was already under way or 'reasonably apprehended' **and**
   the 'dominant purpose' for creating the document was to enable the client's legal adviser to conduct the case or advise the client.

Note: if you forward a lawyer's email to someone else, you may actually waive the legal privilege. Forwarding the email means it's no longer a communication between a lawyer and their client in which advice is sought or provided.

Information cannot be found or retrieved

The information requested is not readily retrievable - section 44(2)(a) - or the information requested does not exist or cannot be found - section 53(a)

An agency can refuse a request if the information is not 'readily retrievable', does not exist or cannot be found, or the agency dealing with the request does not believe that another agency would have the information. Agencies cannot provide what they don't have or can't locate.

Section 44(2(a) provides that a response to a request can notify the requestor that the agency does not hold personal information in a way that enables the information to be readily retrieved.

A request can also be refused if the information requested does not exist or, despite reasonable efforts to locate it, cannot be found.

A lot of information is technically 'retrievable'. For instance, even if information has been deleted from a computer, it can often be retrieved. It may also be difficult to retrieve physical documents particularly if they date back a long way and the records of where they are is not clear. Agencies need to try their best to get information for requesters, but there is only so far that they can reasonably be required to go.

Vexatious, frivolous, trivial

Personal information can be withheld if the request is frivolous or vexatious, or the information requested is trivial - section 53(h)

It's not common to withhold information on this ground. However, it is a protection against requests that are made for malicious or other improper reasons. You cannot use this withholding ground simply because a requester is an annoying or even malicious individual. Unpleasant individuals are still entitled to access their personal information. It is the **request** that needs to be vexatious or frivolous before the information can be withheld.

Information is not personal information about the requester

Under the Privacy Act, people are only entitled to access their own information. Sometimes information requested is simply not information about the requester as it does not identify them in anyway. In this case, you should consider the Official Information Act and reasons to withhold under that law. Inland Revenue is subject to the Official Information Act which covers any information held by a public sector agency. You can find out more about the Official Information Act here.

Out of Scope

Out of Scope

Privacy impact assessments

If you're thinking about starting a project or proposal that relies on personal information (information about an identifiable person), you need to consider privacy implications and risks.

The privacy impact assessment (PIA) is a practical, useful tool to identify whether a project will impact on individuals' privacy or change the way that IR manages personal information.

PIAs help to:

- Identify the potential effects that a proposal may have on people and their information.
- Examine how any detrimental effects might be overcome.
- Ensure that new projects comply with the information privacy principles.

Failure to think about privacy issues when embarking on new projects can be an expensive mistake. PIA's identify opportunities for IR to bake privacy into processes and systems (not bolt it on at the end), which meets best practice. This enables decision makers to get to grips with the issues at the right time - before decisions are taken.

A PIA involves summarising your project, describing the personal information to be used, assessing the project against the privacy principles, and thinking about risk.

A PIA will be a useful part of any change project that:

- Involves information about people or information that may be used to identify or target people.
- May result in surveillance of individuals.
- Will hold or process personal information off-site or off-shore.

Out of Scope

Privacy breaches

Privacy breaches happen when personal information is compromised, usually by being disclosed when it shouldn't have been. Breaches are a reality for all organisations that hold people's personal information and it is vital to IR’s reputation and its relationships with customers that we do everything we can to prevent breaches. This page explains how to report breaches and how IR responds to them.

A privacy breach may occur when one of the principles in the Privacy Act is violated.

The most common breach is when there is unauthorised or **accidental access to personal information or if personal information is disclosed, altered, lost or destroyed**.

A privacy breach only happens when **personal information** is involved and this is defined as **information about an identifiable, living person**. If you disclose information about a company or other organisation, this is not a breach of privacy.

Breaches can happen in a number of ways:

- Personal information being sent to the wrong physical or email address;
- The loss of laptops, mobile devices, USBs or paper records;
- Computers being thrown away or recycled without erasing the contents;

- Databases being hacked or accessed from outside the organisation;
- Employees looking at information outside of their authority;
- Personal information given to a person pretending to be someone else.

It's compulsory that you report a privacy breach if you think one has happened - for instance, if you have sent an email to the wrong person, and the email contained personal information about someone else. We need to know about breaches so we can contain them and prevent them happening again.

Report a breach using the Sensitive Incident notification form (this form is used for reporting privacy breaches or lost/stolen devices).

Notifiable privacy breaches

From 1 December 2020 all agencies in New Zealand have to report notifiable privacy breaches to the Privacy Commissioner and affected individuals.

A **notifiable breach** is a privacy breach that it is reasonable to believe **has caused, or is likely to cause, serious harm** to an affected individual.

When assessing harm we consider:

- the sensitivity of the information (the more sensitive, the higher the risk of harm. A combination of personal information is usually more sensitive than a single piece of personal information);
- size of the breach – how many people can access the information, how many are affected;
- who has the information? Information in the hands of people with unknown or malicious intentions can be of greater risk;
- whether the breach has been contained;
- is the information protected, for example is it encrypted?
- is there a risk of identity theft, fraud or physical harm?
- is there a risk of humiliation or loss of dignity, damage to the individual's reputation or relationships?

You don't have to assess harm but you do have to report a privacy breach using the online form. The Complaints Management Team and Privacy Officer will decide if it's a notifiable privacy breach.

A failure to notify the Privacy Commissioner of a notifiable privacy breach can result in a $10,000 fine.

Responding to and managing a privacy breach

At IR, privacy breaches are logged and managed by the Complaints Management Team with input from the Privacy Officer when necessary. Four key steps should be considered when responding to a privacy breach.

Step 1: Breach containment and initial assessment

- Stop the practice/action.
- Recover the records (if possible).
- Revoke or change computer access (if necessary).
- Ensure evidence is preserved (particularly when information has been stolen).
- Complete the **Sensitive Incident notification form (this form is used for reporting privacy breaches or lost/stolen devices)**.

Step 2**:** Evaluate the risks associated with the breach

- Consider and identify what personal information was involved.
- Establish the cause and extent of the breach.
- Consider who is affected by the breach.
- Identify whether harm could result from the breach.

Step 3: Notification

Decide whether to notify the affected people. If a breach may cause serious harm then we have to formally notify the Privacy Commissioner and affected individuals as soon as possible.

It's not mandatory to notify people of privacy breaches that won't cause harm, but notification is transparent and provides customers with the opportunity to take steps to protect their personal information if necessary, such as by changing passwords or being alert to possible scams resulting from the breach.

Each incident needs to be considered on a case-by-case basis to determine whether notification is necessary. If we do decide to notify, then do it promptly.

It's important that staff engage with individuals who have been affected by a data breach with sensitivity and compassion, in order not to cause them further harm.

However, sometimes notifying individuals can cause undue stress or harm. For example, a breach that poses little risk of harm can cause unnecessary anxiety. Don't notify people unless you're sure whose information has been compromised by the breach. More damage can be done if the wrong people are notified.

If it's a notifiable privacy breach we have to notify the Privacy Commissioner and affected individuals as soon as practicable after becoming aware of the breach.

We should also consider who internally needs to know (the Commissioner or media team for instance) or the Minister's office.

Breach notifications should contain:

- Information about the incident, including when it happened.
- A description of the personal information that has been disclosed.
- Steps taken, or intended to be taken, in response to control or reduce the harm.
- What steps people can take to protect themselves if necessary.
- Contact information for enquiries and complaints.
- Offers of assistance when necessary; for example, advice on changing passwords or a link to Identity Security information.

Apologies

It may be appropriate to apologise for a breach. An apology should acknowledge the hurt or inconvenience caused by Inland Revenue's actions/inactions, and if appropriate, briefly explain the steps taken to prevent the issue from happening again.

There is no apology template as each needs to be considered based on the facts and taking account of the circumstances of the individual(s) affected. However, an apology should be sincere and genuine and acknowledge the mistake. It may include wording such as:

- *This breach/error is regrettable and I apologise that you were one of the affected people.*
- *Inland Revenue takes personal information, privacy and security seriously and it is disappointing we fell short of our high standards when we made this error.*
- *I would like to offer Inland Revenue's sincere apologies for this incident. We regret that this has occurred.*
- *Inland Revenue has notified relevant parties and identified improvements to prevent a similar incident.*
- *We are currently reviewing procedures to ensure an incident of this type does not happen again OR These are the actions Inland Revenue has undertaken to prevent …. happening again.*

If a customer has received information about another individual, you can also say: *Regrettably, you have received information that is not yours and we would like you to return the document. The information was never intended to be sent to you and*

needs to be treated like the valuable lost property that it is. I would ask that you return it in the envelope provided or, if you don't want to return it to Inland Revenue, you could alternatively send it to the Office of the Privacy Commissioner.

Step 4**:** Prevent future breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, investigations are required to determine the cause of the breach and whether or not a prevention plan should be developed.

Privacy incident impact calculator

The Government Chief Privacy Officer has created a calculator to determine the severity of privacy breaches. It can be used to gain insights into privacy practices and culture by assessing the actual and potential impact of its privacy incidents.

The calculator assesses seven areas (including number of individuals affected by the breach, sensitivity of the information and whether the information has been recovered) and determines the impact level from 1 (No Impact) through to 5 (Severe).

You can access the calculator on Digital.govt.nz.

Privacy resources

This page contains links to privacy resources such as training, IR self-assessment reports, policies, guidelines and other related websites.

Out of Scope

Out of Scope

Out of Scope

Out of Scope

- Out of Scope
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

For information about Official Information Act requests, visit the Governance & Ministerial Services site, for Privacy Act requests see the tab above.

Related Links

- Out of Scope
- [redacted]
- [redacted]
- [redacted]
- Governance, Ministerial & Executive Services
- Out of Scope
- [redacted]

External websites

- Office of the Privacy Commissioner
- New Zealand Legislation (links to the Privacy Act 2020)