

---

## MPI Privacy and Transparency Commitment

---

The Ministry for Primary Industries (MPI) understands that the way we use information, particularly personal information, and our overall stewardship of it, directly contributes to the trust and confidence which our stakeholders and the public as a whole have in MPI.

We are accountable for the way we collect, use, store and distribute both personal information (information associated with identifiable individuals, such as someone's name, contact details, address, income, employment details or health status) and non-personal information (information about organisations and businesses, and their practices).

MPI is committed to ensuring the privacy, security, and confidentiality of all the information we hold. This Privacy and Transparency Statement has been developed and published to provide the public and those we engage with in the course of our work with information about the type of information gathering activities we undertake, the purpose of those activities, and the steps we take to manage and protect the information we collect. The statement explains how MPI collects, uses and discloses both personal and non-personal information for regulatory compliance, law enforcement and protective security purposes to keep our staff, and people in New Zealand, and New Zealand safe by:

- preventing, detecting, investigating, responding to and resolving regulatory non-compliance and offending, and
- taking appropriate steps to respond to and mitigate threats to the physical security of people and information, and the security and biosecurity of primary products and places.

### Accessible from this page

1. [Our information governance and assurance framework](#)
  2. [Your privacy and our website](#)
  3. [Information you can provide voluntarily](#)
  4. [Information collection](#)
  5. [Information use and disclosure](#)
  6. [Information we make public](#)
  7. [How we keep personal information safe and secure](#)
  8. [Your rights of access to information we hold](#)
  9. [Concerns or complaints, and enquiries](#)
-

# 1 Our information governance and assurance framework

MPI believes the public deserves to be able to trust public servants to act with integrity. We know the way we handle sensitive and personal information is important in maintaining trust and confidence in what we do and how we do it.

MPI holds a vast amount of data on behalf of New Zealanders. This data is an important strategic asset and is a source of significant value to New Zealand. We acknowledge our obligations to collect, use, manage and disclose the personal information we collect only as provided for by the law, and strive to meet our obligations under the Privacy Act 1993, the Search and Surveillance Act 2012, the New Zealand Bill of Rights Act 1990, MPI's Code of Conduct, and the State Sector Code of Conduct, at all times.

MPI is responsible for administering [legislation](#) that covers a wide range of sectors including, agriculture, [fisheries](#) and [aquaculture](#), [animal welfare](#), [biosecurity](#), [food safety](#), and [forestry](#). For our exporters, MPI's role is to provide trusted assurances to overseas countries that our products meet their requirements. MPI also works with other countries to reduce trade barriers and with importers to prevent unwanted pests and diseases entering the country with imported goods.

Any information gathering, use, sharing or disclosure must be approved according to our relevant internal authorisation processes and procedures which are written and reviewed periodically to ensure compliance with the law, and with our risk management requirements.

MPI also manages data in alignment with the broader open government approach which seeks to ensure transparent government through open data and information that supports a principle of information availability and engagement with government. Through increased access, this data can be used by the private, public, and non-government sectors to drive innovation and contribute to economic, social, and environmental progress. However, as data custodians we look to ensure the protection of interests such as individual privacy, confidentiality and trade sensitivity that can take precedence over wider accessibility.

MPI strongly encourages voluntary compliance across all the areas we regulate. We recognise most people follow the rules and want to comply but there will always be some who don't. For that reason, in certain circumstances we may need to take appropriate action. Our powers and functions therefore extend to the investigation of and resolving possible offences. MPI's information gathering, use and disclosure is governed by a legislative framework that includes the requirements of the legislation we administer, as well as relevant decisions by the courts.

MPI requires all its staff and contractors to adhere to the State Services Commission's Code of Conduct, and to act in a manner that is fair, impartial, responsible & trustworthy. To further strengthen the transparency and accountability of our operations, MPI is committed to adopting and complying with the State Services Commissioner's State Sector [Model Standards](#) for information gathering associated with regulatory compliance, law enforcement and security functions, and to continually strive to improve our proficiency and maturity in accordance with the Government Chief Privacy Officer's core expectations for privacy management and governance in the public sector.

Assurance for staff integrity and conduct within MPI, and for oversight of our regulatory compliance and law enforcement functions, is provided through a number of mechanisms, including through the work of the Security & Privacy Directorate; Human Resources; Procurement; the Assurance and Evaluation Directorate; the Compliance Directorate, the Professional Standards Unit, the Inspector-General for Regulatory Systems, and the Risk and Audit Committee.

## 2 Your privacy and our website

The purpose of this section is to let users of our website know what information we collect when they use the site and why we collect it. It informs you:

- that you can browse our website without providing identifying information
- how we use cookies
- what personal information we collect, use and disclose for specific services (e.g. subscriptions, job applications), for regulatory purposes, or in accordance with the law
- the security of our site and access to information by third parties
- how you can contact us if you have any queries or concerns

### Anonymous information we collect automatically

You can access and browse our website, [www.mpi.govt.nz](http://www.mpi.govt.nz), without disclosing any identifying personal information. We do not automatically record identifying personal information and we do not link information that is recorded automatically with personal information we hold about specific individuals. We do not attempt to identify users or their browsing activities unless they choose to give us personal information.

However, each time you visit our website, and when you read or download information, our system may automatically collect some basic, anonymous, technical information such as:

- the internet address from which you accessed our site (i.e. your domain name; IP address)
- the screen resolution of your PC
- the type of web browser you used to access this site (e.g. Internet Explorer, Google Chrome) and the operating system you use (e.g. Windows 10, Mac OS X)
- the date and time you accessed our website
- the search terms you used to find content on our website
- the pages you accessed, the links you clicked on, and any documents downloaded
- referral data (the last site you visited from which you accessed our website).

We use this information for website management, anonymous analytics and statistical purposes (e.g. to find out what information is used – or not used - and how the site is accessed so we can make it more useful to site users).

### *Cookies and statistical data collected for analytics*

The MPI website uses cookies to temporarily store information in order to enhance your browsing experience (e.g. for managing subscriptions to ensure that only you can change your subscriptions, or to remember the options you selected when using a mobile device).

MPI may also use browser or 'web' cookies to gather data about trends in website usage using a tool called [Google Analytics](#).

Cookies do not collect identifiable personal information. Cookies are small text files placed on your computer's hard drive to collect internet log and user behaviour information in an

anonymous form about how you browse a website. Cookies are used to derive information to help us:

- measure how you use the website so we can update and improve it based on your needs
- remember the notifications you've seen so that we don't show them to you again.

### *Disabling/enabling cookies*

You can manually disable cookies at any time. Disabling cookies will not affect your ability to use this website, but will mean that you can no longer subscribe, manage your subscriptions or unsubscribe online, and you will not get some improved browsing experiences that cookies enable.

If you'd like to enable/disable cookies, in your browser you can do this in:

- Google Chrome > Settings > Show advanced settings > Privacy > Content settings
  - Mozilla Firefox > Options > Privacy > History (Use custom settings for history)
  - Safari > Edit > Preferences > Privacy
  - Internet Explore > Tools > Internet Options > Privacy
-

### 3 Personal information you can provide voluntarily

You may choose to voluntarily provide personal information through this website (e.g. in feedback forms or when making an enquiry or request for information, when subscribing to newsletters, publications and updates, or when completing a form or providing information in relation to a regulated activity).

#### *Subscribing to a service*

When you subscribe to one of our alerts, electronic newsletters or updates, you will be asked to voluntarily provide your name and email address so we can send you the information you've asked for. Where you provide personal information, MPI only uses that information for the purpose or purposes for which it was collected, and only provides it to third parties as specified in this policy or at the point of collection. When you use the "Feedback" form on any of our pages, those messages may be stored and analysed for the purpose of improving our website or services, depending on the nature of the feedback provided.

The information you provide may be viewable by site administrators, certain authorised MPI staff, and contractors (including third parties) providing administrative, maintenance or other services relating to the website. The details you provide may be collected and stored in a secure database by a third party service provider, using its proprietary software, and acting on behalf of the Ministry. At the 'last updated' date below, that third party service provider is [Campaign Monitor](#).

By subscribing to our news and incident alerts you confirm that you give your consent to receive emails from us as defined in the [Unsolicited Electronic Messages Act 2007](#). Subscription to updates is optional and users can unsubscribe at any time by visiting the subscription page for the service you wish to terminate, entering your email address and choosing "Unsubscribe".

If you chose to unsubscribe to our alerts or newsletters at any time, your details will be deleted from the database.

Where we run online forums or similar user-generated discussion sites, information provided by users will be viewable to members of the public using the forum. Should you wish to participate in such a forum, we recommend that you do not disclose any personal information of a sensitive nature through the website.

#### *Online forms*

We may ask or require you to provide some personal information when you complete an online form (e.g. when completing an online feedback form, when registering for a service, or when subscribing to news updates or alerts).

Before you submit certain online forms to us, you'll be asked to confirm that the information you have supplied is true and correct. We record this information securely and use it to update our databases, so it then becomes part of your MPI records.

If you wish to apply for a job with us, you will be required to register your details with us so that we can create an account and maintain a profile for you so we can match your skills and preferences against the job you've applied for (and any upcoming positions if you ask us to), and so we can manage your application. Should your application for a job be unsuccessful, or should you wish to withdraw an application from consideration, your information will be disposed of when our administrative activities are completed.

## *Providing feedback or accessing our "Hot Lines"*

If you make an enquiry or provide feedback to us on our services, and you give us your contact details or phone number, we may use these to respond to your enquiry, to provide the service you have requested, to send you information about our products and services, or to contact you if we require more information from you to meet your needs or to perform our functions.

If you do not provide contact information; you tell us you wish to remain anonymous; or you ask specifically that we do not get in touch, we will not use your email address or other details to contact you, or give them to anyone else unless required to for a lawful purpose.

For example, as a matter of course, we do not share any personal information provided to us through our Hotlines, e.g. the Pest & Disease Hotline (used to report exotic pests/diseases) or the Poacher Hotline (used to report illegal fishing activity). However, should we receive a request under the Official Information Act (OIA) for information collected from a Hotline, an assessment would be made of whether there were grounds to withhold or redact information to remove any personally-identifying information in order to protect the caller's privacy before any information was released.

This approach to redacting any identifying personal information would also be applied to the provision of information to other agencies. For example, if an incoming call to the Hotline provided us with information that indicated we needed to work with other agencies to respond promptly to a potential pest incursion, the nature of the information we needed to share with that other agency would be assessed on a case-by-case basis, and information would only be shared with another agency in a manner consistent with the Privacy Act.

## *Personal information use and disclosure*

We will only use personal information provided to us through this website for the purpose for which you provided it, or a directly related purpose (e.g. to enable us to process a request or investigate a complaint), or for the purposes for which we collected it (e.g. to enable us to administer, evaluate and improve the site, to improve our services, or take action on or respond to the information provided).

We will generally not share personal information that is provided or collected through this website, unless it is necessary to do so for the purpose for which you provided the information to us or for a directly related purpose (e.g. to enable us to investigate a complaint); for the reason we collected it (e.g. in order to administer or improve our website), or where you consent, unless:

- you would reasonably expect information of that kind will be likely to be passed on to other organisations (e.g. companies providing services to or for MPI, or acting on our behalf)
- we consider it is necessary to prevent or mitigate crime (including cyber threats)
- it is otherwise required or authorised by the Privacy Act or any other law (e.g. to prevent offending; for law enforcement; or to prevent or lessen a serious threat to another individual's health or public safety)
- it will be used or published in a way that will not identify you (e.g. in the context of statistical or research work).

## *Cyber security*

MPI websites have security measures in place to prevent the loss, misuse and alteration of information under our control. To maintain the cyber security of our systems and information, our systems are subject to ongoing monitoring (including activity logging), analysis and auditing.

We may use information about your use of our websites and/or other IT systems to prevent unauthorised access or attacks on our systems or to resolve such events. We may use this information even if you are not directly involved in such activity. We may also use services from one or more third party suppliers to monitor or maintain the cyber security of our systems and information. These third party suppliers may have access to monitoring and logging information as well as information processed on our websites and other IT systems. Continued use of MPI websites and/or other IT systems implies acceptance of their use being monitored.

---

## 4 Collection of personal and sensitive information

MPI collects information, including personal and commercially sensitive information, for a range of lawful purposes connected with the exercise of our statutory functions and the activities we undertake to administer the laws we are responsible for. Information may be provided voluntarily, or its provision to us may be mandatory (e.g. where we require information through exercising of our statutory powers).

We may collect information from a variety of sources, including information from:

- individuals
- other agencies or entities (e.g. private sector companies, other New Zealand government agencies, overseas governments and agencies)
- physical sources and locations (e.g. paper records, site visits, inspections)
- technical and scientific devices (including video and audio collection, technical measurement devices and laboratory analyses)
- online sources (including public registers, media reports, websites, and social media).

Open (unregistered) searching of information not subject to personalised privacy settings (e.g. where information can be accessed simply by typing a name or query into a search engine such as Google and no password or account registration or login is required to view information on websites and social media) does not require formal approval for work purposes, including to access and validate information that is publicly available. However, any proposed covert use of social media for verification and investigative purposes to support regulatory, compliance and enforcement work, such as use for active engagement with individuals online without identifying the staff member or the Ministry, is restricted to staff with specialist knowledge, experience and competence, and requires case-by-case approval by relevant senior staff.

### *Information gathered for regulatory and enforcement purposes*

In carrying out our regulatory and enforcement functions (e.g. investigating compliance breaches, taking enforcement action, and determining compliance strategies) the legislation we administer and operate under as a regulator provides us with powers to request or require provision of the information we need to give effect to the legislation (e.g. to assess biosecurity risks when people are coming into the country from overseas).

Where we require information that is relevant to our regulatory and enforcement functions, we may gather information from people or entities using our statutory powers and we may, for example:

- require information to be provided by sworn statement or statutory declaration
- require an original copy of a document to be provided to us
- record an interview conducted in-person or via telephone
- take photographs during site visits or inspections.

### *We collect information directly from you*

We collect information directly from individuals and entities (or their authorised representative) in a number of ways, including when they:

- fill in a form or application either online or in hard copy



- register to use one of our services or subscribe to a newsletter
- contact us by phone, email or by letter, or through an online feedback form
- interact with our staff in the course of their official duties.

In most cases we will tell people (either orally, in writing or in a published privacy statement) why we are collecting information and what we will use it for. In many cases the reason we are collecting information will be obvious because of the nature of a person or entity's interaction with us (e.g. they have made an application under one of the laws we administer, or have asked us to take some action on their behalf).

Where there is a legal requirement for a person or entity to provide specific information (or for us to collect it), we will let them know which law applies and why the information is needed; whether provision of the information is compulsory or voluntary; and what will happen if the information we've asked for isn't provided (e.g. we may not be able to process a request or approve an application).

### *Information collected from a third party (another person or agency)*

In some circumstances MPI collects information, including personal information, indirectly, from other sources, rather than directly from the individual or entity concerned, where it is provided for by law, including where it falls within the exceptions to the privacy principles under section 6 of the Privacy Act. In such circumstances, you may not be aware that we have obtained information about you from another source, particularly if it would prejudice our ability to maintain the law. However, collecting information from a variety of sources can help us identify individuals and businesses who may not be complying with their obligations under the laws we administer and to help us ensure the accuracy of information we hold.

On occasions, external agencies or individuals will provide MPI with information that gives us reasonable cause to believe that the conduct of an individual, or group, might pose a threat to the public or to MPI staff. In such cases MPI may seek assistance of other individuals or agencies (including the Police), or we may collect information from online sources (including websites, social media platforms, and public registers) in a lawful manner, to gain information about individuals or groups of individuals, where we consider it is necessary in order for us to protect our people, information and places.

### *Verification of information before taking action*

When we collect information from third parties, we will take all reasonable and practicable steps to verify the information to ensure it is accurate, relevant and up to date before we use it or pass it on to anyone else. In doing so we take into account a range of factors, including:

- the source of the information (whether it is from an official or unofficial source)
- the credibility and reliability of the source of the information, particularly where it is not an official source;
- the potential impact of the collection, use or disclosure on affected individuals;
- the severity of the harm or impact we are seeking to prevent or address
- the potential impact of the collection, use or disclosure on affected individuals
- the intended and possible outcome(s) of the information collection, use or disclosure (e.g. a potential prosecution or imposition of a fine or other statutory penalty).

### *Information collection to prevent significant harm*

MPI does not employ private investigators to conduct surveillance on individuals. Nor do we engage external security consultants to gather information to support our regulatory compliance and enforcement activities.

However, where we receive advice concerning a direct threat about possible harm to an employee or other individual, MPI will seek to collect the information required to enable us to assess the nature and severity of the threat and the likelihood and severity of the potential harm. In some cases, where information gathering requires specialist capability that we don't have within our organisation, this may involve consultation with an external third party, or engaging them to collect information for us to enable us to assess and address the potential threats to New Zealand or security risks to individuals.

In situations where MPI is seeking to prevent, or address, significant harm we may consider it appropriate to undertake information gathering activity that has an increased impact on an individual. For example, while our statutory officers are generally identifiable by their uniforms or identification, we may collect information by means in which an MPI staff member is not immediately identifiable. This may be necessary where other means of information collection would prejudice an investigation, or otherwise prevent MPI from fulfilling its responsibilities. This includes surveillance activities in accordance with the Search and Surveillance Act 2012.

Collection in these circumstances is subject to enhanced levels of oversight and increased internal controls to ensure it is conducted appropriately. We take care to exercise our information gathering powers lawfully and appropriately, and to meet our obligations under the Privacy Act 1993, State Sector Code of Conduct, and State Services Commissioner's Information Gathering Model Standards at all times.

We protect any information we collect for these purposes and only disclose what we consider is necessary to give effect to our statutory responsibilities, to support other government agencies' law enforcement, regulatory compliance and protective security activities, or otherwise in accordance with the law.

---

## 5 Information use and disclosure

MPI may only use and disclose information in connection with our lawful purposes and functions, and in accordance with relevant legislation, including the Search and Surveillance Act, and the Privacy Act.

We may share information with other government agencies (both in New Zealand and overseas) where necessary in order to properly carry out our legislated functions or to assist another state sector agency fulfil their regulatory compliance, law enforcement, or protective security responsibilities, or to comply with our international obligations and commitments.

This information will only be shared in accordance with our statutory powers, with appropriate caveats and/or controls, and in compliance with the relevant legislation and any information sharing agreements with the other agency. This may include when we are considering and investigating compliance breaches, complaints, and initiating our own investigations or inquiries. We will take all practicable steps to verify information before it is provided to third parties.

We may, for example, share information with:

- another regulator, oversight agency, or complaints body
- the parties to a complaint, for the purpose of investigating and resolving the complaint
- anyone we believe could provide information that is relevant to whether to investigate a complaint, or to an investigation or inquiry, including witnesses to complaint matters
- the Police or another government agency, if required or authorised by law (e.g. to assist with the investigation of a criminal offence), or to report significant misconduct or breach of duty or where there is a serious threat to health or safety. If our staff are threatened or abused, we may refer this to the Police.

Where it is appropriate and practicable you will be made aware of those circumstances as the occasion arises, and if we are able to share that detail with you. Circumstances where we may not advise you of the use or disclosure of your personal information include when we are:

- investigating your behaviour or the behaviour of someone close to you, and it would prejudice our ability to investigate, prevent and detect your or your associates' potential or alleged offending
- sharing with third parties to enable us to investigate or prevent a crime or to progress court proceedings, including where we are applying to Court for a production order or a search warrant
- wanting to prevent or lessen a serious threat to public health or safety or to the life, health or safety of another person or group of people
- assisting another enforcement agency in relation to an investigation or prosecution
- providing intelligence information to other agencies to enable them to maintain the law.

MPI may refer some personal information to contracted providers, or third party non-government organisations where this is required to enable us to perform our lawful purposes and functions. We also share personal information with external agencies contracted to provide services to us, or on our behalf. Where the individual or agency has consented, we

may also use or disclose information we hold to third parties to assist us to communicate or market our services or relevant services of another organisation (e.g. referral to a community support agency or to enable the agency to provide appropriate assistance to MPI or to the individual or agency concerned).

Our procurement processes enable us to include appropriate requirements governing privacy, information security, and commercial confidentiality in our contracts to ensure any third parties working for or with us are bound by the same strict rules that apply to MPI staff.

We may disclose some personal information to other government or non-government agencies through legal mechanisms such as approved information sharing agreements under the Privacy Act, where it is provided for under MPI's or another agency's empowering legislation, and where formalised information sharing arrangements are in place (e.g. the activity is covered by a Memorandum of Understanding or a Cooperation Agreement).

Information may also be provided to, or obtained from, other countries where New Zealand has a treaty arrangement or Cooperation Arrangement, for example, in relation to border security or transnational crime.

We may also be required to disclose information we hold to individuals or organisations in response to requests covered by the Official Information Act 1982 or Privacy Act 1993; to other regulatory agencies or regulators (e.g. to the Ombudsman or Privacy Commissioner in response to a complaint they have received or to support an investigation they are conducting); to a Parliamentary Select Committee or to Parliament in response to a Parliamentary Question; or when it's provided for or required under law or for law enforcement purposes (e.g. when it is necessary to prevent harm being suffered by someone, or where it is necessary to enable MPI or another regulatory or enforcement agency to investigate or prevent a crime), including where the information is subject to a warrant, production order or court order.

In order to carry out our compliance functions, we may use the information we hold for audit or monitoring purposes.

We exchange information for statistical purposes with Statistics New Zealand.

## Information sharing and use for data analytics

In order to carry out our law enforcement, regulatory compliance and protective security functions effectively and efficiently, we may use the information we hold for analysis, risk assessment, audit or monitoring purposes.

MPI also shares information with other agencies who have functions at the border (e.g. the New Zealand Customs Service, the Ministry of Business, Innovation and Technology, and the Department of Conservation, among others). Data analytics helps us gain insights from the information we collect for regulatory purposes to help detect and prevent non-compliance with laws relating to people, goods, craft, mail and trade crossing New Zealand's border. We also use this information to identify hidden connections and patterns to help us target non-compliance, to help with forecasting, to support the work the different border agencies do to reduce border risk, and to develop new ways to help customers comply with their obligations.

Identifiable personal information will only be used where necessary for the intended purposes. No decisions or enforcement actions are taken solely on the basis of the models produced by data analytics.

---

## 6 Information we make public

### *Information published on Public Registers*

Public Registers are lists, registers or databases of information created under a specific piece of law, to which the public has some specific statutory rights of access and where the information contained on the register is open (whether completely or only partially) to public inspection, copying, distribution or search. Some statutory registers open to the public contain no or very little personal information. Those that do contain personal information fall within the personal information protection principles of the Privacy Act 1993. Usually, the legislation that sets up the Public Register will determine what information is on it, who can see it, and what it can be used for.

In administering the legislation we are responsible for, MPI is required by law to publish certain prescribed information on Public Registers. In the case of legislation MPI administers, these include, for example, a number of registers under the Fisheries Act 1996; the Wine Act 2003; the Animal Products Act 1999; the Food Act 2014, and the Agricultural Compounds and Veterinary Medicines Act 1997.

Should any individual have concerns that information made public on a Public Register MPI administers may pose a risk to their safety, or the safety of others (for instance, when there is a domestic protection order in place), they should contact us as in certain circumstances we can take steps to ensure that identifying information covered under the Public Register is not made publicly available.

### *Information included in public submissions*

As well as administering regulations and enforcing compliance, MPI is also a policy agency and we have a role to play in the development of law, as well as its implementation. In that capacity we often consult with the public and seek feedback on proposed changes to practice or law that may impact them. Sometimes we are required by law to consult with potentially affected stakeholders before we make changes to legislation we administer, and at other times we just want to ensure we have the best and most comprehensive information available on which to base our decisions.

Any submission we receive during such consultation becomes official information and copies of submissions can be requested under the Official Information Act 1982 (OIA). The OIA requires us to make submissions available unless we have a good reason for withholding them. We may also choose to proactively publish submissions received to further public discussion and promote transparency in our decision-making.

We therefore ask anyone providing us with information as part of a consultation to let us know if they consider there are reasonable grounds under the OIA to withhold specific information in their submission from public release. Reasons might include that the information contained in the submission is commercially sensitive or personal information. It will remain up to our discretion to decide whether we consider the grounds for withholding the information at issue are reasonable and necessary to protect an interest provided for under the Act. Any decision MPI makes to withhold information can be reviewed by the Ombudsman, who may tell us to release information we have initially decided to withhold.

---

## 7 How we keep personal information safe and secure

We respect your privacy and aim to keep your information confidential unless we are lawfully required or allowed to disclose it.

MPI creates a secure environment for the protection of your personal information and business records. MPI maintains personal and business sensitive information in a number of different databases and information systems. When we collect and store information, we use reasonable security safeguards to protect information from loss, unauthorised access, use or disclosure.

When you provide personal information, it will generally be held by us but may, where it's necessary or most practicable, be stored or accessed on our behalf by authorised third parties (e.g. to administer a database for us). We will store and keep your personal information secure in accordance with the Privacy Act 1993 and any agents working on our behalf will be subject to specified information security and privacy requirements.

All of the information that we hold, whether it is in a digital or hard-copy form, is secured both physically and technically, in accordance with the best and most practicable industry practices that are available to MPI on a commercial basis. In the context of digital information, we use secure servers and any external server providers are scrutinised to ensure we acquire a level of security that adequately protects our infrastructure and information holdings.

We require our staff to use personal information holdings for our business purposes only, and operate on the basis of role-based, needs-only access where possible. All staff are assigned unique passwords. We also implement physical, technical, and organisational measures to prevent unauthorised access, unauthorised or accidental loss, destruction, or damage to your personal information.

The security of both our premises and the information we hold is managed in accordance with the government's [Protective Security Requirements](#) and the [New Zealand Data and Information Management Principles](#).

### How we ensure that personal information is accurate

Before we use personal information or pass it on to anyone else, we will take reasonable and practicable steps to verify the information is accurate, relevant and up to date.

Individuals and businesses should let us know of any change in circumstances such as a change of address to enable us to keep our records as accurate and up to date as possible. You have the right to ask us (either directly or through a representative acting on your behalf) to update your records and to correct any errors or omissions in your personal information that we hold. Where we consider it appropriate to do so, we will update your records. If we do not do so, you may ask us to attach a statement of correction to your records that shows the change requested but not made.

Any action taken based on the information we hold will be proportionate to the level of confidence we have in the information, taking account the source of the information and the context in which we received it (e.g. information provided by a government agency under a formalised information sharing agreement will be considered more likely to be reliable than information received over the phone from an unidentified source).

## How long we keep your personal information

We'll keep your personal information for as long as necessary to achieve the purpose for which we collected it, for the purposes for which the information may lawfully be used, or as required by law.

Any information MPI collects, which may include personal information, (whether collected through use of our website, directly from the individual or organisation concerned, or indirectly from a third party) may be classified as a public record and that information will therefore be retained in accordance with our record retention and disposal policy, to the extent required by the Public Records Act 2005.

---

## 8 Your rights of access to information we hold

All information held by MPI, in any form (e.g. in paper copy or in digital/electronic form) is covered both by the [Official Information Act 1982 \(OIA\)](#) and by the [Privacy Act 1993](#). The OIA and the Privacy Act both help people to participate effectively in government policy decisions and law making and provide for access to information from any person eligible under the provisions of those Acts to make a request.

### Requests for official information

The OIA applies to information about government policies, processes and procedures, and information about individuals other than the requester themselves. Information covered by the OIA includes information about other organisations or people; information about the work we do; are doing, or have done in the past; and information about how we operate as a public sector agency, including our internal rules and procedures and our guidelines for decision making.

### Rights of access and correction for personal information

The Privacy Act covers information we hold that relates to the person making the request. This includes information people give us directly (e.g. when they apply for a permit or make a submission) and information we may have collected from a third party.

### How to request information

MPI has a specialised Ministerials team responsible for managing all OIA and Privacy Act requests. Although any MPI staff member may be asked to assist with preparing a response to a request for information, personal information may only be released after approval by those with formally delegated authority.

If you want to make a request for official information (about what we do or how we do it, including where it involves other people), contact us at [info@mpi.govt.nz](mailto:info@mpi.govt.nz).

If you want to ask about or access personal information we may hold about you, contact us at [privacyrequests@mpi.govt.nz](mailto:privacyrequests@mpi.govt.nz)

Whether you are making a request for information covered by the Official Information Act or the Privacy Act, to ensure we can respond to your requests as quickly and efficiently as possible, please make sure you include with your request:

- your name and whether you are asking for information on behalf of yourself, another person (that is, you have authority to act on their behalf) or an organisation
- an outline of the information you're wanting
- your contact details so we can respond to your request and get in touch with you if we need further information about what information you're after.

We may ask you to identify yourself if you aren't known to the person responding to the request. In such cases we may need to sight a primary and secondary form of identification, one of which includes a photograph of you. If you are an agent acting on behalf of an individual or business, we will also require you to provide evidence that you have authority to act on their behalf.



We will usually allow you to have access to the information that we hold about you, in the way that you prefer, unless there is good reason to the contrary. The nature of the information we hold means we may also responsibly withhold information from release in accordance with grounds set out in the Privacy Act or OIA, as may apply.

We will always attempt to provide you with access to your information in a timely manner, and we will always aim to respond to an information request within 20 working days of its receipt. However, we will let you know if we think we will need more time to respond. The time it will take us to identify information relevant to your request; to assess whether it can be released or should be withheld; and to prepare and send a response, will always depend on the nature and complexity of your request; the volume of information we have to access, collate and consider; and how recently we collected the information and where it is held (e.g. on a readily accessible electronic database or in off-site storage or in our archives). We will let you know if we consider we'll need an extension of the timeframe for responding (e.g. due to the scope of the request or where there is a need for us to consult other parties before we can make a decision on the request) and we will let you know when we expect to be able to reply. If we refuse a request, we will let you know why and the steps you can take if you do not accept our decision and want it to be reviewed.

### How to request correction of information

You have the right to ask us to correct the information we hold if you think it is not correct.

The law permits us to decline to correct information if we don't believe the requested change is appropriate. However, if we have a good reason for refusing a request for correction, you can ask that a statement be attached to the information describing the change asked for that was not made.

---

## 9 Concerns, complaints, and enquiries

At MPI we're committed to providing you with excellent and timely service. If you aren't satisfied with our service or processes; you think we have fallen short in terms of the way we have performed our statutory functions; or you disagree with a decision we've made in relation to a request for official information or for personal information, you have the right to make a complaint to the [Ombudsman](#) or the [Privacy Commissioner](#).

More information on the process for making a request or lodging a complaint can be found on the [Ombudsman's Office](#) or [Privacy Commissioner's](#) websites.

However, before you consider making a formal complaint about how we've handled things, we'd like the opportunity to understand the basis for your complaint and put things right where we can. So if you have any concerns, please contact our team at [complaints@mpi.govt.nz](mailto:complaints@mpi.govt.nz).

Alternatively, any concerns or questions about privacy-related matters can be raised, in confidence, with our Chief Privacy Officer, at [CPO@mpi.govt.nz](mailto:CPO@mpi.govt.nz), or by post by writing to PO Box 2526, Wellington 6140, New Zealand.

### Where to go for further information

Should you have any general questions regarding this statement or want further information, you can contact us at [info@mpi.govt.nz](mailto:info@mpi.govt.nz). You can also call us on **0800-00-83-83** if you are in New Zealand, or **+64-4-830-1574** if you are calling from overseas.

Last reviewed: Date 28 June 2019

Has this been useful? [Give us your feedback](#)

---