



Privacy Policy

Guidelines and procedures

| | |
|-------------------------------------|---|
| Policy owner | Chief Legal Advisor |
| Policy approved by | The WorkSafe Board |
| Policy reviewed and approved | 13/12/2021 |
| Next review due | 13/12/2023 |
| Distribution | This policy will be published on the WorkSafe New Zealand website and intranet. |

This policy is provided to all staff and Board members. It is the responsibility of each staff and Board member to understand and apply this policy. It also applies to contractors engaged by WorkSafe. It is the responsibility of the Manager engaging the contractor to ensure they comply with all WorkSafe policies while working for WorkSafe.

Position statement

This policy support's WorkSafe's compliance with the requirements of the Privacy Act 2020.

Purpose/Overview

This privacy policy sets out the principles which are used by WorkSafe to collect, store, use and disclose personal information.

Scope

WorkSafe is New Zealand's primary work health and safety regulator and the regulator for electricity and gas safety in the workplace and home. In our role we work closely with PCBUs, workers, and others to educate them about work health and safety, engage them in making changes that reduce the chances of harm, and enforce the legislation for which we are responsible. WorkSafe collects, holds and uses personal information in order to fulfil our regulatory role and also as part of employing and engaging staff.

WorkSafe is committed to ensuring that personal information is managed appropriately and we strive to uphold good practice privacy standards in the collection, storage, use, and disclosure of personal information.

Personal information at WorkSafe is subject to:

- The [Privacy Act 2020](#) and associated [13 Information Privacy Principles](#) (external link) that cover the collection, handling and use of personal information
- The [Official Information Act 1982](#)
- The [Public Records Act 2005](#).



Policy statements

1. Information Privacy Principles

The collection, storage, use and disclosure of personal information is governed by the Privacy Act. In particular, section 22 sets out 13 information privacy principles (IPPs). WorkSafe must comply with these IPPs. Many of the IPPs have exceptions to them, therefore it is important to refer to the requirements in full in the Privacy Act when considering their scope, but below is a summary:

- **IPP 1:** WorkSafe must only collect personal information if it is necessary for a lawful purpose connected with a function or activity of WorkSafe
- **IPP 2:** WorkSafe must only collect personal information directly from the individual concerned, or their appointed representative
- **IPP 3:** When it collects the information, WorkSafe must take reasonable steps to ensure the individual knows it is being collected, the purpose of the collection and who will see it
- **IPP 4:** WorkSafe must collect personal information by lawful means and in a fair and reasonable manner
- **IPP 5:** WorkSafe must use reasonable safeguards to protect personal information against loss, unauthorised access, use, modification or disclosure, and any other misuse
- **IPP 6:** Individuals are entitled to request access to personal information that is held about them
- **IPP 7:** Individuals are entitled to request that the information held about them be corrected
- **IPP 8:** WorkSafe must take reasonable steps to ensure that the personal information is accurate, up to date, relevant, and not misleading before using it
- **IPP 9:** WorkSafe must not keep the information for longer than needed for the purposes for which it may lawfully be used
- **IPP 10:** WorkSafe must not, in most cases, use personal information obtained in connection with one purpose for another purpose
- **IPP 11:** Personal information held by WorkSafe must not, in most cases, be disclosed to another person or organisation
- **IPP 12:** WorkSafe must not disclose personal information to a foreign person or entity that is not subject to the Privacy Act or comparable safeguards, unless WorkSafe has obtained authorisation from the individual concerned
- **IPP 13:** WorkSafe must not assign a unique identifier to an individual unless it is necessary to carry out its functions, and must not use a unique identifier issued to a person by another agency.

2. Creation and collection of personal information:

WorkSafe will collect information only for purposes that are linked to our functions or activities, and will collect it in a way that is fair and reasonable.

WorkSafe will, unless there is a lawful reason not to, make people aware of the collection of information, our purposes for doing so, and their rights to access and correct that information.

3. Storing of personal information

WorkSafe will maintain all reasonable safeguards against the loss, misuse or inappropriate disclosure of personal information, and maintain processes to prevent unauthorised use or access to that information. In particular:

- WorkSafe will keep physical documents secure when there is a business need to take them outside of WorkSafe premises, and no technical solution is applicable.
- WorkSafe will keep electronic personal information secure by ensuring its data storage is protected from external sources, maintaining regular back up of data to secure storage and applying good practice for information security management.
- WorkSafe may use cloud computing services to manage and store information. Where used, WorkSafe will ensure that cloud computing services meet all applicable government security requirements.

4. Requests for personal information

WorkSafe will provide individuals with access to their personal information, where appropriate, and respect the individual's right to seek amendment of factually incorrect information.

Requests for information will be processed by WorkSafe in accordance with its Privacy Act Guidelines. In particular WorkSafe will:

- Acknowledge a request for personal information or correction of information as soon as possible after receipt.
- Respond to requests for personal information, or correction of personal information, as soon as is reasonably practicable (and within 20 working days of the request being made unless extended under the Privacy Act).
- Notify the requestor, in the case of a request for correction of personal information, whether the information has been (or will) be corrected, and if not, the requestor's right to provide a statement of correction to be attached to the information.

5. Use of personal information

WorkSafe uses personal information to fulfil its functions including promoting and contributing to a balanced framework for securing the health and safety of workers and workplaces and promoting the safe supply and use of electricity and gas. WorkSafe will use personal information only for the purposes for which it is collected, except where legislation allows it to be used for other purposes. WorkSafe will, when using information, take reasonable steps to ensure it is complete, relevant, up to date and not misleading.

WorkSafe will not use personal information in its user training or systems testing, unless in a form that does not identify the individual(s) concerned.

6. Information sharing and disclosure of personal information

WorkSafe may share information externally where it is lawful to do so. For example, WorkSafe may disclose information to other agencies where there is an express legislative authority or requirement to do so. In addition, the Privacy Act allows the sharing of personal information to facilitate the provision of public services in accordance with approved information sharing agreements (AISAs). An AISA is a formal agreement under Part 7 of the Privacy Act, and WorkSafe may consider entering into an AISA where it is satisfied that it would facilitate the more effective provision of public services and where applicable legal requirements are satisfied.



WorkSafe may also disclose personal information to other agencies where it believes on reasonable grounds that it falls within one of the exceptions to IPP 11 of the Privacy Act.

7. Third party arrangements

Where WorkSafe enters into arrangements with third parties that involve the use or management of personal information held by WorkSafe, appropriate provisions will be included to protect that personal information.

Where WorkSafe holds personal information on behalf of another agency there may be specific contractual or statutory requirements that WorkSafe must also comply with.

The requirements for third party arrangements need to be considered on a case by case basis.

8. Privacy incidents

A privacy incident includes an actual privacy breach, a potential privacy breach, or a near miss.

A privacy breach occurs when there is an unauthorised or accidental access to, or disclosure, alteration, loss or destruction of personal information. A privacy breach can also include an action that prevents the agency from accessing the information on either a temporary or permanent basis.

A potential privacy breach occurs where a privacy breach may have occurred, but it is not known if an actual breach occurred.

A near miss is where an action could have resulted in a breach but ultimately the breach does not occur.

All privacy incidents (actual and potential breaches or near misses) discovered by staff should be notified to their immediate manager. Managers are responsible for managing the response to the privacy incident in accordance with WorkSafe's Privacy Incident Guidelines.

WorkSafe's Privacy Incident Reporting form should be completed as soon as possible. This will be provided to WorkSafe's Privacy Officer who will advise further on the management of the privacy incident. This may include notifying the incident to the Office of the Privacy Commissioner where required under the Privacy Act or if notification is considered necessary in the interests of transparency.

Complaints

Where any member of staff becomes aware of a privacy complaint made by an individual to WorkSafe or to the Office of the Privacy Commissioner, WorkSafe's Privacy Officer should be notified.

Further obligations

WorkSafe will:

- Train and inform its employees and contractors of this policy and ensure the information privacy principles are applied when fulfilling their role within WorkSafe
- Endeavour to protect the privacy of staff members
- Regularly review WorkSafe business processes that relate to the collection, access, use, storage and destruction of personal information so they remain relevant and reflect good practice.

Who to contact

WorkSafe's Privacy Officer can be contacted at PrivacyOfficer@worksafe.govt.nz.

Responsibilities

| Position | Responsible for |
|---|---|
| All WorkSafe staff (including contractors), Board and Committee members | Complying with this policy, in particular by: <ul style="list-style-type: none">• Being aware of and complying with this policy as relevant to their role• Undertaking any necessary training• When identified, reporting any privacy concerns, issues or risks, or failures to comply with this policy |
| WorkSafe Board | Approval of this policy and oversight of WorkSafe's compliance with it |
| Executive Leadership Team | Monitoring to ensure compliance |
| Chief Legal Advisor | Privacy Officer for WorkSafe |
| Privacy Officer | Monitoring to ensure compliance Monitoring and supporting the investigation and resolution of privacy incidents Reporting notifiable privacy breaches to the Office of the Privacy Commissioner |
| Manager Digital Workplace | Supporting privacy through: <ul style="list-style-type: none">• promotion of appropriate data and information management governance practices• providing operational support and guidance |
| General Manager People, Culture, and Safety | Supporting training requirements regarding privacy as appropriate |
| Managers | Ensuring staff are aware of the existence of this policy |



| | |
|--|--|
| | <p>Monitoring compliance of staff with this policy</p> <p>Investigating and managing the response to any privacy incidents in accordance with WorkSafe’s Privacy Incident Guidelines</p> |
|--|--|

Related documents

[Privacy Act](#)

[Official Information Act](#)

[Public Records Act](#)

Privacy Act Guidelines

Privacy Incident Guidelines