Privacy

Introduction

When to use

Use this policy when you want to understand the requirements for collecting, storing, handling and using personal information at Fire and Emergency New Zealand when we are not operating in an emergency.

Note: Application of the Information Privacy Principles (IPPs) may differ when Fire and Emergency is operating in an emergency situation.

This policy should also be used when managing a privacy incident or making a privacy complaint, in conjunction with the Managing privacy incidents guidelines or Making privacy complaints guidelines.

Note: You should read this policy in conjunction with Te Tikanga Whanonga Our Code of Conduct and Unacceptable behaviours schedule.

Contents

This policy contains the following content:

About this policy

Purpose

This purpose of this policy is to set expectations for ensuring that Fire and Emergency only collects personal information for a lawful purpose, safely and securely stores personal information, and ensures personal information is not used or disclosed for unauthorised purposes. It is also to ensure individuals are protected from any harm that could result from breaches of the Privacy Act 2020.

This policy sets out expectations for those that collect, hold, use or disclose personal information so that Fire and Emergency complies with the responsibilities set out in the Privacy Act 2020. That is, we treat the personal information we collect and hold lawfully, respectfully and with care, and only use or disclose personal information where permitted. The purpose of this policy is also to ensure that privacy incidents and complaints are managed appropriately.

This policy also sets expectations in relation to persons requesting access to their personal information and taking reasonable steps to update personal information when it is wrong.

Who it applies to	We expect the following groups of people to comply with this policy: • permanent and temporary employees • casual employees • volunteers • contractors (individuals, employees of contractors, subcontractors, or persons affiliated with third parties) • anyone working on behalf of Fire and Emergency (for example, service providers). In some cases, our providers will have their own privacy policy, however, when these providers are delivering services on our behalf, the requirements of this policy will apply instead. Everyone has a duty to meet the commitment and requirements statements below.

Definitions

The following definitions apply to this policy and all places where these terms are used in Fire and Emergency:

Personal information	Personal information means any information about an identifiable individual. The Privacy Act 2020 applies to all personal information collected and held by Fire and Emergency. Personal information includes information about people in our community, and information about Fire and Emergency employees and volunteers or individuals who provide services on behalf of the organisation. Examples of personal information include names, addresses and contact details, and also location of incidents if they occurred on private property.
Sensitive personal information	Sensitive personal information is information about an individual that has some real significance to that person, is revealing of them, or generally relates to matters an individual might want to keep private. This includes information that will potentially allow others to draw inferences about the individual, or might result in the individual being treated a certain way. Examples of sensitive personal information include information about a person's race, ethnicity, gender or sexual orientation, health, disability, age and religious, cultural and political beliefs.

Policy statements

Our commitment	At Fire and Emergency, we're committed to respecting the information we collect and hold about other people and ensuring we treat it lawfully and with care. Everyone at Fire and Emergency deals with information in some way, including personal information about people, which can be sensitive, such as the identities of victims involved in emergency incidents. The communities we serve have a right to expect that we will respect their privacy and comply with our legal obligations.

Requirements	As personnel of Fire and Emergency, we are responsible for ensuring the collection, use, disclosure and storage of any personal information complies with the IPPs in the Privacy Act 2020. Further detail on the IPPs is provided below, and guidance is also available on the Office of the Privacy Commissioner's website at privacy.org.nz > Privacy Act 2020 > Privacy Act 2020 and the Privacy Principles.
Minimising risk	Fire and Emergency will consider the IPPs each time a system or process that collects, uses, discloses and/or stores personal information is reviewed, adapted or developed. The Privacy Officer must be engaged at the outset of any new initiative to determine whether a Privacy Impact Assessment (PIA) is required.
Privacy Impact Assessments (PIA)	A Privacy Threshold Assessment must be completed at the outset of any new initiative or project to determine whether a Privacy Impact Assessment (PIA) is required. There is more information about completing a PIA on the Office of the Privacy Commissioner's website at privacy.org.nz > Your responsibilities > Privacy Impact Assessments.
Privacy incidents	All privacy breaches and near misses (collectively known as privacy incidents) regarding unauthorised access to, correction of, use of or disclosure of personal information must be reported to the Privacy Officer. Privacy incidents will be managed according to the Privacy incident process in the *Managing privacy incidents guidelines*. Under this process, the Privacy Officer or the Legal Team will take steps to: • contain the breach and perform an initial assessment (contain) • initiate an investigation, and evaluate the risks (evaluate) • remedy and respond (notify) • consider the cause and how to prevent it happening again (prevent). The Privacy Officer will engage with and inform the Privacy Commissioner of notifiable privacy breaches when appropriate and required to by law. Privacy incidents will be recorded by the Privacy Officer and reported on regularly to Audit and Risk Committee of the Fire and Emergency New Zealand Board. The Information and Communications Technology (ICT) Directorate may also be involved in this process, in particular, when the incident involves a security breach.
Privacy complaints	Privacy complaints will be assessed, investigated and responded to according to the process set out in the *Making privacy complaints guidelines*. The Privacy Officer will provide advice, assistance and oversight in the management of privacy related complaints. Where the complaint is identified as a breach, the privacy incident process set out in the *Managing privacy incidents guidelines* will also be followed. Privacy complaints will be recorded by the Privacy Officer and reported on regularly to the Audit and Risk Committee of the Fire and Emergency New Zealand Board.

Commitment to Māori

At Fire and Emergency, we are committed to working with Māori as tangata whenua.

Fire and Emergency, through implementing our Rautaki Māori, will consider tikanga and te ao Māori when collecting, storing, using or disclosing personal information that relates to Māori. Fire and Emergency will also engage with Māori when making decisions that relate to Māori personal information.

Good information privacy practice at Fire and Emergency

Introduction

The Privacy Act 2020 sets out the Information Privacy Principles (the IPPs). The IPPs are the basis for good information privacy practices. If we follow these principles, it will mean that Fire and Emergency is acting lawfully in our collection, use, disclosure and storage of personal information

Information Privacy Principles

The following table summarises the IPPs.

Note: For general information, see the Office of the Privacy Commissioner's guidance at privacy.org.nz > Privacy Act 2020 > Privacy Act 2020 and the Privacy Principles.

IPP number	Principle
IPP 1	Only collect personal information if it's necessary for a lawful purpose and connected with Fire and Emergency's functions or activities.
IPP 2	Where possible, always collect personal information directly from the person.
IPP 3	Be open and transparent with people about why we're collecting their personal information.
IPP 3A	If you collect personal information other than from the individual concerned, you must take reasonable steps to ensure the individual is aware their personal information has been collected and certain information about the collection.
IPP 4	Ensure personal information is collected fairly, reasonably and legally.
IPP 5	Keep personal information safe and secure.
IPP 6	Let the person see their information if they ask to see it
IPP 7	Correct personal information if we're asked to do so
IPP 8	Ensure personal information is accurate and up to date before it is used.
IPP 9	Dispose of personal information when it is no longer needed and lawful to do so.
IPP 10	Only use personal information for the purpose for which it is collected or if there is another valid reason.
IPP 11	Only disclose personal information if it directly relates to the purpose for which it was collected or there is another valid reason. For information requests during an emergency, see Requesting information from Fire and Emergency New Zealand in emergencies guideline.
IPP 12	Only disclose personal information overseas if there are appropriate safeguards in place.
IPP 13	Only use unique identifiers where it is clearly allowed.

Integrating privacy into organisational processes	Privacy management must be considered at the initiation stage when developing, updating or upgrading any of Fire and Emergency's systems and processes. A Privacy Impact Assessment will usually be required before developing, updating or upgrading systems and processes.
Collecting and storing personal information (IPPs 1–5)	When collecting information, Fire and Emergency must be clear and open about our purposes for collecting personal information, limit the intrusiveness of collection and keep the personal information secure. Fire and Emergency will: • only collect information that is necessary and relevant to Fire and Emergency's functions, and only collect the minimum information necessary • wherever possible, collect personal information directly from the person or people concerned • be as open as possible about why the information is being collect, the intended use of the personal information collected, and who will have access to the information • be clear about whether providing the information is compulsory or voluntary, and what will happen if the information isn't provided • collect personal information in a way that respects individuals' personal needs for privacy • ensure personal information held by Fire and Emergency is safe and secure • protect personal information held by Fire and Emergency from loss, unauthorised access, use, modification or disclosure, or other misuse. **Note:** During an emergency, there are different rules around collecting and gathering information under IPPs 2–4. For example, during an emergency, Fire and Emergency can collect and gather relevant information about a property without the property owner's consent. At any other time, we would require consent from the property owner to collect information about the property.
Accessing and correcting personal information (IPPs 6–7)	Fire and Emergency must facilitate requests from individuals to view and correct their personal information. Fire and Emergency will: • give people access to their personal information if it is readily retrievable, unless a withholding ground under the Privacy Act applies • tell people that have requested their information that they are entitled to request that we correct the information, if it is wrong • make every effort to correct personal information on request **Note:** If we are not willing or able to do this, an individual is entitled to require us to attach a statement to the information setting out the corrections they have asked for. • ensure requests to access personal information are referred to the Information Requests Team at officialinformationrequests@fireandemergency.nz.

Using and disclosing personal information (IPPs 8–13)

Fire and Emergency must manage personal information carefully, including only using or disclosing personal information with proper authorisation or where use or disclosure is permitted under the Privacy Act. Personal information should only be kept as long as needed for the purposes for which it was collected.

Fire and Emergency will:

- take reasonable steps to check personal information is accurate, up to date, complete, relevant and not misleading before using the information
- only retain personal information if it is still needed for the purpose for which it is collected.

  Note: Before disposing of any records or information including personal information, you **must** contact the Records Management Team to ensu e disposal is lawful and complies with the Public Records Act 2005.
- only use personal information for the purpose it was collected, unless an exemption applies
- only disclose person information with authorisation, unless it is necessary to disclose the information for one of the purposes for which it was collected, or one of the exemptions in the Privacy Act applies
- only disclose personal information to another organisation outside New Zealand if the receiving organisation meets one of the following criteria:
  - They are subject to the Privacy Act because they do business in New Zealand.
  - They are subject to privacy laws that provide comparable safeguards to the Privacy Act.
  - They have agreed to adequately protect the information (for example, by using model contract clauses).
- only use unique identifiers where it is necessary to enable Fire and Emergency to carry out its functions.

Note: If another organisation is requesting personal information from Fire and Emergency in an emergency, follow the Requesting information from Fire and Emergency New Zealand in emergencies guidelines.

Responsibilities

Table of responsibilities

Individual and collective responsibilities are assigned in the following table:

Role	Responsibilities
Fire and Emergency Executive Leadership Team	Lead and model best practice behaviours to ensure privacy is core to all aspects of the culture within Fire and Emergency
Deputy Chief Executive Office of the Chief Executive	• Consider privacy matters escalated from the Privacy Officer to the Deputy Chief Executive Office of the Chief Executive • If matters are not resolved, then escalate the matter to the Chief Executive for consideration
Privacy Officer	• Work with relevant business units to ensure effective privacy risk management is fully embedded within the risk management activities of Fire and Emergency • Ensure resource is available to support compliance activities with this policy and associated guidelines

	• Ensure organisational controls are in place to support the implementation of this policy • Develop and provide training and communications to raise awareness of this policy and build capability in good privacy practice • Oversee privacy investigations and complaints • Regularly report on privacy incidents, investigations and complaints • Notify any notifiable privacy breaches to the Privacy Commissioner and the individuals affected
Legal Directorate	• Provide legal advice in relation to compliance with the Privacy Act 2020 and associated codes and regulations • Provide legal advice in relation to information-sharing arrangements • Assist with investigations and complaints involving privacy issues • Prepare Privacy Impact Assessments (as and when that is appropriate and necessary)
Information and Communications Technology Directorate	• Ensure privacy has been appropriately considered before making or allowing technology changes • Address privacy concerns within their capability and capacity
Data and Analytics Directorate	• Ensure Person Private Information (PPI) data stored within the Modern Data Platform and our Geospatial platform has been appropriately identified as private information, and has metadata which describes it • Ensure that those accessing PPI from our data platforms are doing so appropriately • Ensure Privacy Impact Assessments are completed and current for all data sets stored on our data platforms • Manage the appropriate sharing of PPI with third party organisations, including other emergency services partners
Records Management Team	• Oversee the disposal of Fire and Emergency information, including personal information, to ensure it is in line with Public Records Act 2005 requirements • Provide advice and support on the secure storage of personal information within their capability and capacity
Managers and Supervisors at all levels and all locations	• Identify privacy risk in their own teams and ensure appropriate controls are in place • Notify privacy incidents to their own manager and the Privacy Officer • Liaise with the Privacy Officer following all privacy incidents • Ensure personnel are aware of their obligations regarding personal information and recognise the importance of their role in privacy • Ensure new personnel complete privacy training as appropriate • Model good privacy behaviour – take due care in managing and working with personal information • Take steps as advised by the Privacy Officer (or the Legal Team on behalf of the Privacy Officer) following a privacy incident
All personnel (as described in Who it applies to above)	• Treat information with care and respect • Report all privacy incidents to a manager and the Privacy Officer • Comply with this policy • Understand and apply this policy and the Information Privacy Principles (IPPs) in their day-to-day work • Refer to privacy guidance and seek advice from the Privacy Officer when needed • Actively participate in privacy training

Related information

Who to contact:

If you have questions about this policy or to make a privacy complaint, email the Privacy Officer at PrivacyOfficer@fireandemergency.nz

Policies

Te Tikanga Whanonga Our Code of Conduct

Unacceptable behaviours schedule

Vetting

Guidelines

Managing privacy incidents

Making privacy complaints

Requesting information from Fire and Emergency New Zealand in emergencies

Legislation

Privacy Act 2020

References

Privacy Act 2020 and the Privacy Principles

Document information

Owner	DCE Office of the Chief Executive
Steward	Privacy Officer
Last reviewed	4 June 2025
Review period	Yearly

Record of amendments

Date	Brief description of amendment
April 2022	Initial version.
10 July 2024	Standards of Conduct policy retired and replaced by the Te Tikanga Whanonga Our Code of Conduct, and Unacceptable behaviours schedule. No further review, no version update.
4 June 2025	Scope of policy widened to include collection, storage and security of personal information, added additional definitions, expanded explanation of IPPs and how Fire and Emergency will comply with the IPPs.
3 November 2025	Added Vetting policy to Related information. Not reviewed.