Requesting information from Fire and Emergency New Zealand in emergencies

Introduction

When to use

These guidelines apply to situations where:

- a significant emergency has occurred, is occurring or may occur; and
- another Government agency requests information from Fire and Emergency New Zealand relating to that emergency that might include 'personal information', as defined in the Privacy Act 2020.

Example: A request from Civil Defence Hawke's Bay for CAD data (111 call data) in anticipation of a major weather event that may cause significant damage.

These guidelines are intended for use by both the agency requesting the information and the relevant Fire and Emergency personnel responding to the request.

Role

- Incident Commanders
- Coordination Centre personnel
- Geospatial personnel
- Government Agencies seeking data from Fire and Emergency

Contents

Overview

When to follow the process

This guide outlines the process for requesting information from Fire and Emergency that potentially includes 'personal information' as defined in the Privacy Act 2020.

Information privacy principle (IPP) 11(1)(f) in section 22 of the Privacy Act 2020 allows for the disclosure of personal information where it can be shown that the disclosure of that information is necessary to prevent or lessen a serious threat to:

- public health or public safety; or
- the life or health of the individual concerned or another individual.

Key principles

1. Requests must comply with IPP 11(1)(f) of the Privacy Act 2020.
2. The threat must be 'serious' as defined in the Act.
3. Disclosure must be necessary to prevent or lessen the serious threat.
4. Only the minimum amount of information necessary should be requested.

Understanding 'serious threat'

A 'serious threat' under the Privacy Act 2020 is determined by considering:

- the likelihood of the threat being realised
- the severity of the consequences if the threat is realised
- the time at which the threat may be realised.

Privacy principle 11 – Limits on disclosure of personal information

Privacy principle 11

Privacy principle 11 (IPP 11) is a key principle in section 22 of the Privacy Act 2020 that sets out the rules for when an agency can disclose personal information to other parties.

The general rule is that an agency should not disclose personal information unless one of the specified exceptions applies. These exceptions cover various scenarios where disclosure might be necessary or justified, such as when the disclosure is one of the purposes for which the information was collected, when the individual concerned authorises it, or in certain situations involving law enforcement or public safety.

Privacy principle 11(1)(f)

IPP 11(1)(f) specifically deals with the disclosure of personal information in situations involving serious threats. It states:

> An agency that holds personal information must not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,— ...
>
> (f) that the disclosure of the information is necessary to prevent or lessen a serious threat to—
>
> (i) public health or public safety; or
>
> (ii) the life or health of the individual concerned or another individual

IPP 11(1)(f) provides a crucial exception for agencies like Fire and Emergency to share information if they believe, on reasonable grounds, that the disclosure is necessary to address serious threats to public or individual safety.

This exception recognises that there may be emergency situations where the need to protect public safety or an individual's life or health outweighs the general principle of keeping personal information private. However, the threat must be 'serious', and the disclosure must be necessary to prevent or lessen that threat.

Privacy principle 9 – Agency not to keep personal information for longer than necessary

Privacy principle 9 (IPP 9)

When agencies receive personal information from Fire and Emergency under IPP 11(1)(f), they must comply with IPP 9 of the Privacy Act 2020, which requires that personal information is not kept longer than necessary for the lawful purpose for which it is being used.

Time-bound nature of emergency information	Information shared during emergencies or to address serious threats is inherently time-sensitive. The retention period should align with: • the duration of the serious threat • the time required to prevent or lessen the threat • any statutory requirements for record-keeping.
Determining appropriate retention periods	When requesting information, agencies must consider: • the expected duration of the serious threat • the time required for any immediate response actions • any follow-up activities required • statutory record-keeping requirements.
Destruction requirements	When the retention period ends: • Securely destroy or return all copies of the information. • Document the destruction/return process. • Provide written confirmation to Fire and Emergency, including details of any copies provided to third parties and their destruction.
Exceptions to standard retention	Any need to retain information beyond the resolution of the serious threat must be: • clearly justified • documented • communicated to Fire and Emergency • supported by a legal basis.

Steps for government agencies to request information from Fire and Emergency

	Agencies requesting information from Fire and Emergency are required to follow these steps:
1. Identify the serious threat	You must be able to: • clearly describe the nature of the threat • explain why it qualifies as ‘serious’ considering likelihood, severity and timeframe (how imminent it is).
2. Establish necessity	You must be able to: • explain how the requested information is necessary to prevent or lessen the threat. • demonstrate why other means of addressing the threat are insufficient.

3. Determine the specific information needed	Fire and Emergency can provide the following types of data under IPP 11(1)(f): • Computer Aided Dispatch (CAD) data • Wide Area Assessment (WAA) data and imagery • Rapid Disaster Assessment (RDA) data and imagery • Drone captured imagery • Hazardous Substance location data • Other data sets not described above Consider carefully which of these data sets are necessary to address the serious threat – please see 'Appendix 1: Data definitions' for more details.
4. Complete the request form	Use the official 'Request for personal information from Fire and Emergency New Zealand' form. Provide all required information, including: • Your agency's details • Specific information requested (use the checkboxes provided) • A detailed description of the serious threat • Justification for why the disclosure is necessary • An explanation of why obtaining the individual's authorisation is not practicable or desirable • Urgency of the request. For urgent threats, explain why it is urgent. • Proposed method for secure transfer of information • Information retention statement
5. Ensure proper authorisation	The request should be made by an authorised officer of your agency. Include your position and authority to make the request.
6. Submit the request	• For urgent threats, clearly state the urgency and reasons. • Send the completed form to gis-support@fireandemergency.nz, attention Chief Data and Analytics Officer.
7. Follow-up	• Be prepared to provide additional information if requested by Fire and Emergency. • Fire and Emergency will assess the request against IPP 11(1)(f) and may seek clarification if needed.

Important considerations for agencies requesting information

When requesting information	• Be specific about the information you need. Check only the relevant data set boxes. • Clearly demonstrate how the threat meets the criteria for a 'serious threat'. • Explain why it's not practicable or desirable to obtain the individual's authorisation. • Ensure you have measures in place to protect any information disclosed to you.
After receiving information	• Use the information only for preventing or lessening the stated serious threat. • Securely store and handle the information.

Fire and Emergency assessment process

Basis of assessment	Fire and Emergency will assess any request for information that potentially includes personal information based on: • adequacy of the description of the serious threat • necessity of the disclosure to prevent or lessen the threat • impracticability or undesirability of obtaining individual authorisation • legitimacy and scope of the request. Fire and Emergency reserves the right to decline any request for information if, in Fire and Emergency's opinion, disclosure of that information is not justified under IPP 11(1)(f) or if Fire and Emergency has concerns about the ability of the agency concerned to use, manage or store that information in accordance with the Privacy Act 2020.
Contact	For any questions about this process, please contact the Chief Data and Analytics Officer: gis-support@fireandemergency.nz

Remember: Protecting individuals' privacy is a shared responsibility. Always consider the privacy implications of your request and handle personal information with care, even in threat situations.

Appendix 1: Data definitions when requesting information from Fire and Emergency in emergencies

Introduction

Overview

This document provides detailed information about the datasets that may be requested from Fire and Emergency New Zealand. It includes descriptions of each dataset, the specific information contained within, and details on how the data will be provided or accessed.

Definitions

Computer Aided Dispatch (CAD) data

Description

CAD data contains real-time and historical information about emergency incidents, resource allocation and response times.

Information included and excluded

Included:

- Event type
- Date, time and location of incident

Excluded:

- Responding units and personnel
- Response times (dispatch, en route, arrival, departure)
- Incident updates and notes
- Caller information (name, contact details, location)

Format and access

Preferred method:

- Access provided by dedicated GIS web portal – Fire and Emergency ArcGIS Online (AGOL) account to the recipient AGOL account, using the AGOL sharing group system.

Alternative methods (may be subject to capacity constraints to deliver):

- Provided as CSV or Excel files
- GIS exports of CAD data (Shapefile, KML)
- Historical data may be provided via requestors secure file transfer (SFTP)

Wide Area Assessment (WAA) data and imagery

Description

WAA data includes comprehensive assessments of large areas affected by disasters or major incidents, often including oblique imagery and damage assessments.

Information included and excluded

Included:

Imagery and location specific data across in the following areas:

- Pre-impact reconnaissance
- Impact tracks
- Impacted property/infrastructure
- Impacted routes
- Hazards
- Incident ground facilities
- Animals

Excluded:

The following data sets are not included by default and special requests are required to access the follow data sets.

- Immediate risk to life
- Targeted search required

Format and access

Preferred method:

- Access provided by dedicated GIS web portal – Fire and Emergency ArcGIS Online (AGOL) account to recipient AGOL account, using the AGOL sharing group system.

Alternative methods (may be subject to capacity constraints to deliver):

- Provided as CSV or Excel files
- GIS exports of CAD data (Shapefile, KML)
- Historical data may be provided via requestors secure file transfer (SFTP)
- Imagery provided in standard formats (JPEG, TIFF or GeoTIFF)

Rapid Disaster Assessment (RDA) data and imagery

Description

RDA data provides quick, initial assessments of disaster-affected buildings and properties, focusing on immediate impacts and urgent needs.

Information included and excluded

Included:

Imagery and location specific data included are:

- Preliminary property/building damage assessment
- Oblique (ground) imagery of affect properties and buildings

Format and access

Preferred method:

- Access provided by dedicated GIS web portal – Fire and Emergency ArcGIS Online (AGOL) account to recipient AGOL account, using the AGOL sharing group system.

Alternative methods (may be subject to capacity constraints to deliver):

- Provided as CSV or Excel files
- GIS exports of CAD data (Shapefile, KML)
- Historical data may be provided via requestors secure file transfer (SFTP)
- Imagery provided in standard formats (JPEG, TIFF or GeoTIFF)

4. Drone captured imagery

Description

High-resolution imagery and video captured by drones during or after an incident, providing detailed visual information about specific areas or structures

Information included and excluded:

Included:

- High-resolution photographs
- Video footage
- Thermal imaging data (if applicable)

Format and access

Preferred method:

- Access provided by dedicated GIS web portal – Fire and Emergency ArcGIS Online (AGOL) account to recipient AGOL account, using the AGOL sharing group system.

Alternative methods (may be subject to capacity constraints to deliver):

- Images provided in high-resolution formats (JPEG, TIFF)
- Videos in standard formats (MP4, AVI)
- Historical data may be provided via requestors secure file transfer (SFTP)

5. Hazardous Substance Location Data

Description

Information about the storage, handling and transportation of hazardous substances within Fire and Emergency's jurisdiction.

Information included and excluded:

Included:

- Location of hazardous substance storage sites
- Types and quantities of hazardous substances

Format and access

Preferred method:

- Access provided by dedicated GIS web portal – Fire and Emergency ArcGIS Online (AGOL) account to recipient AGOL account

Alternative methods (may be subject to capacity constraints to deliver):

- Safety data sheets and response plans as PDF documents
- Historical data may be provided via secure file transfer (SFTP)

Notes on data provision and access

1. All data will be provided in a secure manner.
2. Large datasets may be split into multiple files or provided through a series of secure transfers.
3. Real-time or near-real-time data may require setting up special access protocols, which will be arranged on a case-by-case basis and at the requestor's cost.
4. Fire and Emergency may require the requesting agency to have specific software or technical capabilities to access certain data formats, particularly for GIS data.
5. In all cases, Fire and Emergency will work with the requesting agency to ensure that data is provided in a usable format while maintaining necessary security protocols.

For any questions about data formats, access methods or technical requirements, please contact gis-support@fireandemergency.nz

Document information

Owner	Chief Data and Analytics Officer
Steward	Manager Data and Analytics Capability
Last reviewed	5 February 2025
Review period	Every second year

Record of amendments

Date	Brief description of amendment
February 2025	Initial version