Pagers
Privacy Impact Assessment

13 December 2021

1. Project summary

1.1 Brief description of the project

This Privacy Impact Assessment (**PIA**) relates to Fire and Emergency's current use of pagers. Pagers are communication equipment used by Fire and Emergency New Zealand (**Fire and Emergency**) personnel as part of the incident response process. In particular, pagers are used by the Communication Centre (**ComCen**) to send messages to personnel to alert them of a new incident and to provide information for additional situational awareness.

1.2 General overview/Personal information

a. The purpose of pager messages is to alert personnel of an emergency requiring a turn out. The information communicated on pagers usually contain two key pieces of information, being property address and type of incident (ie fire, medical). Pagers are a reliable form of communication, and have better coverage particularly in alerting personnel in rural areas.

b. Executive officers, and other specific response roles (such as fire risk management roles) can also use pagers for messaging throughout the incident. The type of information could be an updated situation report from the fire ground.

c. Pagers operate on an analogue network and are not encrypted. 9(2)(a) 9(2)(c)

9(2)(a) 9(2)(c)

d. Pagers do not require a log-in (unlike some other electronic devices). This means that when it receives an alert, it is possible for someone else who is near the pager to simply pick it up and read the message.

e. This is a review of the current use of pagers, so that its current risks can be taken into account when Fire and Emergency considers any change to its communication equipment.

1.2 Personal information involved

The table below sets out the following:

- the personal information that will be collected, used and/or disclosed
- the source of the information
- the purpose of the information for your project.

Note: "Personal information" is any information about an identifiable living person. However, a person doesn't have to be named in the information to be identifiable.

Type of personal Information	Source of Information	Purpose of information
Information communicated on pagers		
Details of the incident / turnout information, usually including: • property address of the incident; • type of incident. It is very rare for individual's names to be communicated on pagers.	ComCen: • who receives the information from the 111 emergency caller; • who may carry out additional research to provide information to personnel to assist with the incident response.	To perform Fire and Emergency's function, including to provide response to fire and other incidents.

2. Privacy assessment

2.1 Areas that are risky for privacy

Some types of projects are commonly known to create privacy risks. If the project involves one or more of these risk areas, it's likely that a PIA will be valuable.

Use this checklist to identify and record whether your proposal raises certain privacy risks. Delete any that do not apply.

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
Information management generally			
A substantial change to an existing policy, process or system that involves personal information ***Example***: *New legislation or policy that makes it compulsory to collect or disclose information*		✓	This assessment is regarding the existing way Fire and Emergency uses pagers.
Any practice or activity that is listed on a risk register kept by your organisation ***Example:*** *Practices or activities listed on your office's privacy risk register or health and safety register*		✓	No.
Collection			
A new collection of personal information ***Example:*** *Collecting information about individuals' location*		✓	This assessment is regarding the existing way Fire and Emergency uses pagers. No new or additional information is proposed to be collected other than what is already collected to respond to incidents.
A new way of collecting personal information ***Example:*** *Collecting information online rather than on paper forms*		✓	This assessment is regarding the existing way Fire and Emergency uses pagers.
Storage, security and retention			
A change in the way personal information is stored or secured ***Example:*** *Storing information in the cloud*		✓	This assessment is regarding the existing way Fire and Emergency uses pagers.

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
Transferring personal information offshore or using a third-party contractor ***Example:*** *Outsourcing the payroll function or storing information in the cloud*		✓	
A decision to keep personal information for longer than you have previously ***Example:*** *Changing IT backups to be kept for 10 years when you previously only stored them for 7*		✓	
Use or disclosure			
A new use or disclosure of personal information that is already held ***Example:*** *Sharing information with other parties in a new way*		✓	
Sharing or matching personal information held by different organisations or currently held in different datasets ***Example:*** *Combining information with other information held on public registers, or sharing information to enable organisations to provide services jointly*		✓	
Individuals' access to their information			
A change in policy that results in people having less access to information that you hold about them ***Example:*** *Archiving documents after 6 months into a facility from which they can't be easily retrieved*		✓	
Identifying individuals			
Establishing a new way of identifying individuals ***Example:*** *A unique identifier, a biometric, or an online identity system*		✓	

Does the project involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
New intrusions on individuals' property, person or activities			
Introducing a new system for searching individuals' property, persons or premises ***Example:*** *A phone company adopts a new policy of searching data in old phones that are handed in*		✓	
Surveillance, tracking or monitoring of movements, behaviour or communications ***Example:*** *Installing a new CCTV system*		✓	
Changes to your premises that will involve private spaces where clients or customers may disclose their personal information ***Example:*** *Changing the location of the reception desk, where people may discuss personal details*		✓	
New regulatory requirements that could lead to compliance action against individuals on the basis of information about them ***Example:*** *Adding a new medical condition to the requirements of a pilot's license*		✓	
List anything else that may impact on privacy, such as bodily searches, or intrusions into physical space	✓		Pagers operate on an analogue network and are not encrypted. 9(2)(a) 9(2)(c) 9(2)(a) 9(2)(c) In addition, pagers do not require a log-in (unlike some other electronic devices). This means that when it receives an alert, it is possible for someone else who is near the pager to simply pick it up and read the message, which may contain personal information.

2.2 Privacy Act 2020

The current use of pagers raises compliance risks in respect of information privacy principle 5 in the Privacy Act 2020. These are considered further in the table below, along with other information privacy principles.

Description of the Privacy Principle	**Summary of personal information involved, use and process to manage**	**Assessment of compliance**
Principle 1 – purpose of collection Collect personal information only for a lawful purpose	Information is collected for the purpose of responding to incidents.	The purpose of collecting the information is in line with Fire and Emergency's functions and objectives. No compliance. issues with the purpose of collection.
Principle 2 – source of information Collect information directly from the person it is about, or if not possible then collect it from other people in certain circumstances	Personal information include details of the incident, such as: • type of incident • property address of the incident; The source of information is the ComCen, who receive information from the 111 emergency caller. The emergency caller may not be calling about themselves or their own property.	Receipt of information from 111 callers includes unsolicited information, and principle 2 does not apply to unsolicited receipt of information. However, the ComCen will likely also collect information from callers once they are engaged on a call. In so far as this information includes personal information, it is not always collected from the person that the information is about. For example, a member of the public may call about a fire at another property or about another person trapped in a motor vehicle. However, non-compliance with this principle can be justified for one or more of the following reasons: (1) non-compliance would likely not prejudice the interests of individuals concerned. (2) Compliance would prejudice the purposes of the collection. (3) non-compliance is necessary to prevent or lessen a serious threat to the life or health of the person concerned, or another person. (4) Compliance is not reasonably practicable in the circumstances of the particular case.

Description of the Privacy Principle	Summary of personal information involved, use and process to manage	Assessment of compliance
Principle 3 – what to tell an individual Take reasonable steps to make sure person knows why it is being collected, who will receive it, what happens if information is not given	Individuals call 111 to report an incident either about themselves, or about other individuals or other property.	No compliance issues in relation to principle 3, but noting that: • Insofar as the information is collected from the individual concerned, the nature of the means of collection (during a 111 call) means that it would not be reasonably practicable to provide all the detail required by privacy principle 3(1) and doing so is likely to prejudice the interests of the individual concerned insofar as it could delay an emergency response. • Personal information is not always collected from the individual concerned, as such it is not possible to comply with principle 3 in those situations.
Principle 4 – manner of collection Only collect information in ways are that lawful	Some of the information will be provided through unsolicited communication and some will be collected from 111 callers by ComCen.	For information that is collected by ComCen, there is no concern that this is not collected lawfully, unfairly or in an unreasonably intrusive manner.

Description of the Privacy Principle	Summary of personal information involved, use and process to manage	Assessment of compliance
Principle 5 – Storage and security of personal information Secure personal information against unauthorized access, use, modification or disclosure and other misuse.	Pager messages are stored so they can be used for fire investigation reports, Coroner investigations, and potentially information requests from the public. The pager messages contain limited information which is usually provided elsewhere i.e fire investigation reports. As such, we understand there have been no requests for pager messages. However, the data is important as it shows the fact that pager messages were sent and what time they were sent. The pager messages are stored securely on iCAD, and can only be accessed through that system in ComCen by relevant personnel. Pagers operate on different channels, and those codes are required to be known in order for Comcen to send messages to pagers. Comcen can choose the code and direct the messages to be sent to certain personnel. However, messages appearing on pagers are not encoded or password protected and can be viewed by anyone looking at the pager.	The current storage/access system appears to be sufficiently robust/secure. No concerns of compliance as to storage and security of personal information (ie the pager messages which may contain personal information). However, there are concerns as to compliance due to the potential for unauthorised access. Pagers operate on an analogue network and are not encrypted. 9(2)(a) 9(2)(c) 9(2)(a) 9(2)(c) Pagers do not require a log-in (unlike some other electronic devices). This means that when it receives an alert, it is possible for someone else who is near the pager to simply pick it up and read the message, which may contain personal information. In accordance with Fire and Emergency's ICT Acceptable Use Policy, personnel are required to store mobile devices in a secure environment eg access-controlled Fire and Emergency premises, whenever it is not under direct supervision, and that devices are not to be left unattended in plain view or in high-risk places, such as airport terminals or in clear sight in a vehicle.
Principle 6 – Access People have the right to access their personal information. There are some reasons to refuse access Principle 7 – Correction A person has a right to ask for their information to be corrected	Principles 6 and 7 require that an individual be able to have access to, and request correction of, their information.	Fire and Emergency has other processes in place to provide for this – ie through official information request channels.

Description of the Privacy Principle	Summary of personal information involved, use and process to manage	Assessment of compliance
Principle 8 – Accuracy Before using or disclosing personal information, make sure it is accurate, and not misleading	Personal information must not be used or disclosed without taking reasonable steps in the circumstances to ensure it is accurate and up to date. The information will be used or disclosed contemporaneously with its provision to ComCen.	Given that the information will likely be disclosed contemporaneously with its provision to Comcen, there are no issues with compliance with this principle.
Principle 9 – Retention Personal information must not be kept for longer than necessary	Records of the messages sent on pagers are potentially kept indefinitely because it is kept on the the iCAD system. The pager messages are stored so they can be used for fire investigation reports, Coroner investigations, and potentially information requests from the public.	Pager messages are unlikely to be needed indefinitely, and a policy regarding the disposal of pager messages is recommended. However, pager messages are likely kept indefinitely because it is kept in iCAD. Recommend that the disposal policy for pager messages may be better considered against iCAD generally. The same information (ie type of incident and property address) is also stored in SMS reports. The disposal policy for pager messages can also be considered against any policies regarding SMS reports.
Principle 10 – Use Information should only be used for the purpose it is collected	The information collected is used by ComCen to provide information in order for Fire and Emergency to respond to incidents, such as to alert personnel and provide turn out information.	There is no concern that personal information is used for a purpose than which it is obtained. Use for purposes other than responding to the particular incident would potentially breach the Privacy Act 2020. Any proposal to use the information for a different purpose should be discussed with legal first.
Principle 11 – Limits on disclosure of personal information Only disclose it if you've got a good reason, unless one of the exceptions applies	Pager messages and related pager information (such as the fact that a pager message was sent, and the timing of the message) may be included in reporting, such as SMS reports. SMS reports may be provided to other organisations (ie the Coroner) or members of the public through information requests.	Fire and Emergency has other processes in place to provide for the proper disclosure of information – ie through official information request channels.

Description of the Privacy Principle	Summary of personal information involved, use and process to manage	Assessment of compliance
Principle 12 – Cross-border disclosure Personal information can only be sent overseas if the information will be adequately protected	The information is not known to be disclosed outside of New Zealand. The information is stored by Police, rather than Fire and Emergency, and they are responsible for compliance with principle 12 insofar as information may be stored overseas.	Likely no compliance issues.
Principle 13 – Unique identifiers Only assign unique identifiers where it is necessary for operational functions	No knowledge that unique identifiers are assigned with the use of pagers or their voice recordings.	No compliance issues as unique identifiers are not used in relation to pagers.

2.3 Initial risk assessment

If you answered "Yes" to any of the questions above, use the table below to give a rating – either **Low (L)**, **Medium (M)**, or **High (H)** – for each of the aspects of the project set out in the first column. If you answered "No" to all the questions in 2.1 above, move on to section 3 below.

For risks that you've identified as Medium or High, indicate (in the right-hand column) how the project plans to lessen the risk (if this is known).

Aspect of the Project	Rating (L, M or H)	Describe any medium and high risks and how to mitigate them
Level of information handling L – Minimal personal information will be handled M – A moderate amount of personal information (or information that could become personal information) will be handled H – A significant amount of personal information (or information that could become personal information) will be handled	L/M	Potentially a low-medium amount of personal information may be handled (ie sent through as a short form message on pagers). It is noted that it is very unlikely that people's names will be included in pager messages. The message would include type of incident and property address, and this would require information to be pieced together to link the information shared on pagers with an individual. It may also be very difficult to link the information to a specific individual if there are multiple people occupying the address. Risks of unauthorised access can be mitigated through: 1. 9(2)(a) 9(2)(c) 2. using cellphones for messaging instead of pagers, for parts of the country and roles where this is possible; 3. encryption – if this is possible. Measures should be taken to mitigate risks of unauthorised access to personal information. It is however important to keep in mind that pagers are important communication equipment for incident response, so any measure taken must not negatively affect Fire and Emergency's ability to respond to emergencies/incidents.

Aspect of the Project	Rating (L, M or H)	Describe any medium and high risks and how to mitigate them
Sensitivity of the information (e.g. health, financial, race) L – The information will not be sensitive M – The information may be considered to be sensitive H – The information will be highly sensitive	L/M	Personal information that is shared on pagers may be sensitive but will be at a very high level if it is. The information shared on pagers is property addresses and nature of the incident. It is possible for someone who knows who occupies the property to link information to the individuals. This is something that is more likely to occur in smaller communities where a person picks up a responder's pager, knows who lives at the address identified and can look online to understand what kind of incident the code refers to. Measures should be taken to mitigate risks of unauthorised access to personal information. It is however important to keep in mind that pagers are important communication equipment for incident response, so any measure taken must not negatively affect Fire and Emergency's ability to respond to emergencies/incidents.
Significance of the changes L – Only minor change to existing functions/activities M – Substantial change to existing functions/activities; or a new initiative H – Major overhaul of existing functions/activities; or a new initiative that's significantly different	L	There are no changes. This assessment is regarding the existing way Fire and Emergency uses pagers.
Interaction with others L – No interaction with other agencies M – Interaction with one or two other agencies H – Extensive cross-agency (that is, government) interaction or cross-sectional (non-government and government) interaction	L	Pagers are an internal process and equipment, and are not used to interact with personnel from other agencies.

Aspect of the Project	Rating (L, M or H)	Describe any medium and high risks and how to mitigate them
Public impact L – Minimal impact on the organisation and clients M – Some impact on clients is likely due to changes to the handling of personal information; or the changes may raise public concern H – High impact on clients and the wider public, and concerns over aspects of project; or negative media is likely	H	Changes to pagers would have a high impact on Fire and Emergency's response to incidents, and would have scope to affect the public (who relies on Fire and Emergency to respond to incidents). Pagers are important communications equipment, and they are a crucial piece of equipment to communicate with personnel particularly in rural areas.

3. Summary of privacy impact

The privacy impact for this project has been assessed as:	Tick
Low – There is little or no personal information involved; or the use of personal information is uncontroversial; or the risk of harm eventuating is negligible; or the change is minor and something that the individuals concerned would expect; or risks are fully mitigated	
Medium – Some personal information is involved, but any risks can be mitigated satisfactorily	✓
High – Sensitive personal information is involved, but any risks can be mitigated satisfactorily	
Very high – Sensitive personal information is involved, and several medium to high risks have been identified	
Reduced risk – The project will lessen existing privacy risks	
Inadequate information – More information and analysis is needed to fully assess the privacy impact of the project.	

3.1 Reasons for the privacy impact rating

There is potential for a low to medium amount of personal information to be shared on pagers.

Personal information shared on the pagers may be sensitive, as it includes property addresses and the nature of the incident. It will be possible for someone who knows who occupies the address to link the nature of the incident to the individual or individuals concerned. This is more likely to occur in smaller communities than in major centres.

Unauthorised access to view the pager messages is relatively easy because:

1. Pagers operate on an analogue network and are not encrypted. 9(2)(a) 9(2)(c) 9(2)(a) 9(2)(c)

2. Pagers do not require a log-in (unlike some other electronic devices). This means that when it receives an alert, it is possible for someone else who is near the pager to simply pick it up and read the message, which may contain personal information.

The more likely risk is that an unauthorised person picks up and looks at a responder's pager and already knows who occupies the address that is identified. Fire and Emergency's ICT Acceptable Use Policy already includes requirements for personnel to keep mobile devices secure. Compliance with this policy will mitigate this risk of unauthorised access.

4. Recommendation

A medium privacy impact rating has been assessed. This is due to the potential for information shared on pagers to be accessed by unauthorised members of the public, and for that information to be linked to individuals by people who know who occupies the address identified. There are risks as to unauthorised access to the information 9(2)(a) 9(2)(c)

These risks may be able to be mitigated through:

(1) using cellphones for messaging instead of pagers, for parts of the country and roles where this is possible;
(2) encryption if this is possible for pagers;
9(2)(a) 9(2)(c)
(4) ensuring personnel appropriately manage their pagers and do not leave them where unauthorised members of the public can pick them up and review messages. In accordance with Fire and Emergency's ICT Acceptable Use Policy, personnel are required to store mobile devices in a secure environment eg access-controlled Fire and Emergency premises, whenever it is not under direct supervision, and that devices are not to be left unattended in plain view or in high-risk places, such as airport terminals or in clear sight in a vehicle.

Measures should be taken to mitigate risks of unauthorised access to personal information. It is however important to keep in mind that pagers are an important communication tool for communication with personnel so any measure taken must be not negatively affect Fire and Emergency's ability to respond to emergencies/incidents.

5. Sign off

9(2)a

Cindy Colenbrander
Legal Counsel

13 / 12 / 2021
Date