

19 September 2024

Joshua Rogers
fyi-request-28036-92d535f5@requests.fyi.org.nz

Tēnā koe Joshua

Request for information

Thank you for your Official Information Act 1982 (OIA) request dated 13 August 2024, in which you asked:

Please provide all documentation for vGrid.

*User Manual
Training documentation
Privacy policy
Privacy impact assessment*

And provide any further information police hold on vGrid

Please note that the part of your request that asks for '*any further information police hold on vGrid*' has been excluded from this response as per the refined request that was received from you on 19 August 2024.

In response to parts 1 and 2 of your request, enclosed are the vGRID SaferCity Platform User Guides which encompass User Manual and Training documentation.

In response to part 3 of your request, enclosed is the latest version of the vGRID Privacy Policy which is publicly available on the SaferCities website: <https://vgrid.io/privacy/platform>

In response to part 4 of your request, as Police are committed to openness and transparency, we sometimes proactively release information and documents that may be of interest to the wider public. A privacy impact assessment on Police use of Automatic Number Plate Recognition (ANPR) platforms, including vGRID, has been made publicly available and can be found on the New Zealand Police website - [Proactive information releases | Police use of emergent technologies | New Zealand Police](#). Enclosed is also the SaferCities Brief Privacy Analysis documents and their Privacy Impact Assessment in relation to vGRID VAULT.

Please note that references to a 30-day vGRID VAULT retention period in documents released for parts 1, 2 and 4 of the response was a placeholder and is currently under review.

Police National Headquarters

180 Molesworth Street. PO Box 3017, Wellington 6140, New Zealand.
Telephone: 04 474 9499. Fax: 04 498 7400. www.police.govt.nz

Please also note that some information has been withheld within the documents provided in response to parts 1, 2 and 4 in accordance with the following sections of the OIA:

- 6(c) - in that the making available of this information would be likely to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences, and the right to a fair trial
- 9(2)(b)(ii) - in that the making available of this information would likely unreasonably prejudice the commercial position of the person who supplied or who is the subject of the information.

You have the right to ask the Ombudsman to review my decision if you are not satisfied with the response to your request. Information about how to make a complaint is available at: www.ombudsman.parliament.nz.

Yours sincerely

A handwritten signature in black ink, appearing to read 'M. P. Winter', with a long horizontal flourish extending to the right.

Matt Winter
Executive Director – Chief Information Officer
New Zealand Police

VGRID

SaferCity Platform Police User Guide

2 May 2024 – v3.0



Table of Contents

vGRID SaferCity Platform Overview	1
Who are SaferCities?	2
Requesting access to vGRID	3
Support for vGRID.....	3
How to access vGRID via a Police Enterprise PC.....	3
Adding the vGRID App to your Police Mobility Device.....	4
vGRID Streams Overview	5
Streams Functions bar	6
vGRID ANPR Overview	7
What is ANPR?	7
vGRID ANPR	7
Privacy & Policy	7
Alerts	8
Alerts View	9
Alerts Notifications	10
Quick Search.....	11
Search & Export	12
Plates Of Interest.....	14
Insights	16
Real-time	16
vGRID Vault Overview	17
Vault Cases Dashboard.....	17
Vault Request Files	18
Vault Upload Files	20

Who are SaferCities?

Collaborating with an ecosystem of agencies, companies, and communities, we provide independent consulting and the vGRID SaferCity Platform, to connect customers physical CCTV and ANPR back to police, emergency services, and themselves in a secure way.

Through this ecosystem approach, our mission is to improve public safety, create vibrant communities and safer cities.

We also provide smart, secure, managed networking services with specialist messaging technology, to enable people to nominate and connect their public facing CCTV cameras to police and emergency services.

SaferCities have developed and maintained the vGRID SaferCity platform for Police in NZ since 2015. We also serve as valued consultants to law enforcement agencies in New Zealand and Australia, holding Master Services Agreements to deliver specialised services. SaferCities has comparable agreements with local authorities, councils and commercial entities.



SaferCities CEO Scott Bain, and CTO Chris Wiggins receiving a Certificate of Appreciation from Commissioner Mike Bush and Superintendent Richard Chambers for providing Police real-time access to community CCTV in May 2016.

vGRID SaferCity Platform Overview

The vGRID SaferCity Platform is software for Police. It provides access to live and historical information. This includes live CCTV cameras, operator screens, and vehicle number plate reads (ANPR).

The platform also includes vGRID Vault, providing Police with the ability to request digital files from victims and witnesses. Members of the public can then be sent a link which allows them to upload evidence (video, images, or other), allowing the Police to receive evidence digitally without a physical visit.

This guide is designed for use on Desktop/Laptop devices. Not all of the functions highlighted below are available for mobile users.



Respond

Investigate

STREAMS
Live video

CCTV Cameras
Specialist screens

ANPR
Database

Live alerts
Historic search

Vault
Evidence request

Request digital files
from the public

Requesting access to vGRID

If you are unable to log into vGRID using your NZ Police email and password or to request additional permissions, please email our support inbox with the following details:

- 'Access to vGRID' in the email title
 - Physical location
 - Workgroup
 - Reason for access
-

Support for the vGRID Platform

For any vGRID related enquiries, please visit our online user guide and FAQ's using the links below. Alternatively, contact us via phone or email using the details provided.

F.A.Q - docs.vgrid.io/faq

Email - support@safercities.com

Phone - 09 281 9777

How to access vGRID via a Police Enterprise PC

1. Using a NZ Police computer, open vGRID using the linked provided:

- **s.6(c) OIA**

2. Log in using:

- `firstname.lastname@police.govt.nz`
- Your Police Enterprise password

vGRID SaferCities

NEW ZEALAND POLICE

vGRID is integrated with Police Enterprise

Please sign in with your Police email address
eg: first.last@police.govt.nz

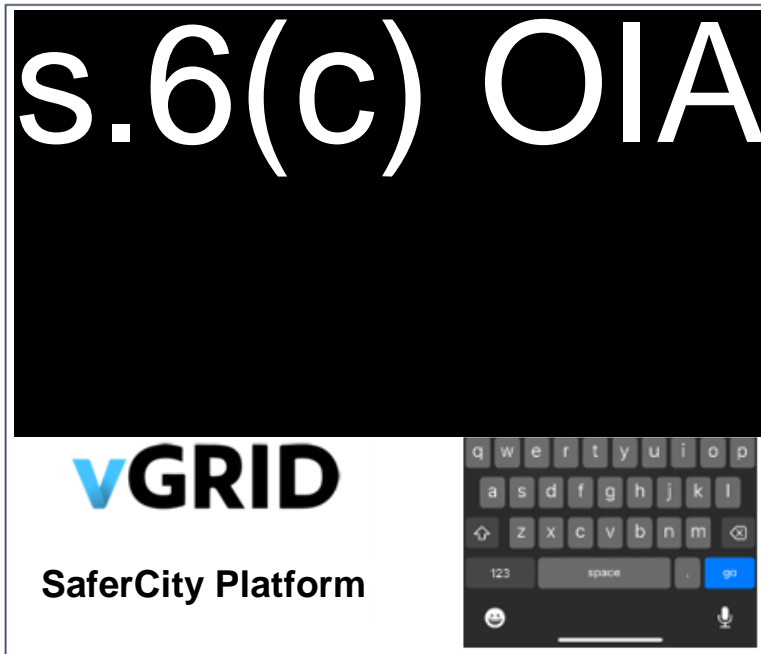
Sign in

Email (first.last@police.govt.nz)

Can't access your account? [Next >](#)

Adding the vGRID App to your Police Mobility device

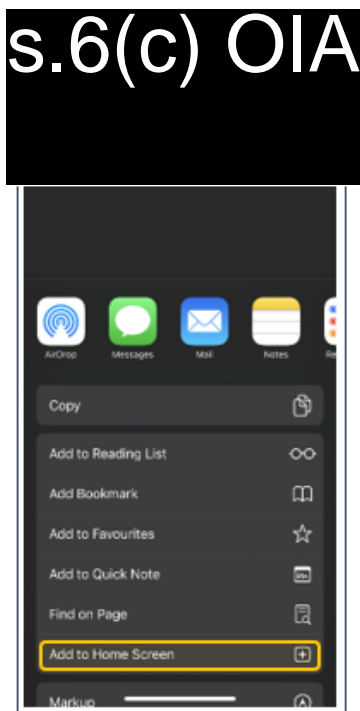
1. Navigate to **s.6(c) OIA** (or scan QR Code) using Safari on your Police Mobility Device.



2. Open the 'Share Panel' (Bottom Middle)



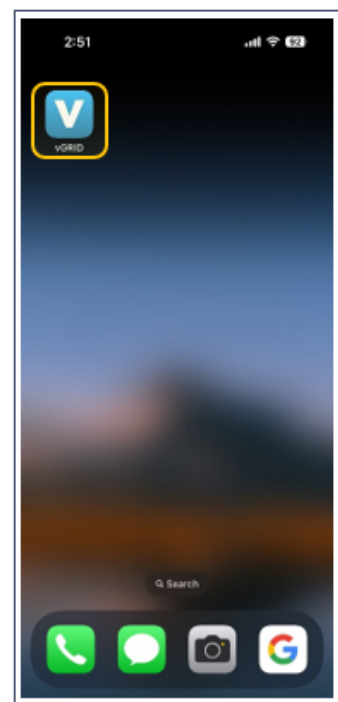
3. Scroll down the sharing options and select 'Add to Home Screen'.



4. Click Add.



5. A vGRID Link will now appear on your home screen.










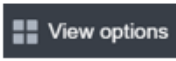
vGRID Streams Overview

Streams enables Police access to live CCTV video or CCTV operator screens from authorised public agencies and commercial/private entities via vGRID.

Streams are assigned based on the users location and role. Specialist streams can be requested, however these require additional approval. For example: Eagle requires approval from the TM Metro Operations manager.

s9(2)(b)(ii)

1.  **Site groups**
Indicates an area containing several sites. Clicking on this will expand it to show all sites within the group.
2.  **Sites**
Indicates a site or preset containing multiple cameras.
3.  **Offline camera**
Indicates a camera that is currently offline and cannot be viewed
4.  **Active camera**
Indicates a camera that is active and can be viewed by double clicking the name or dragging it onto the screen.

5.  **Search bar**
Enables users to search for a camera by or site.
6.  **Camera map**
This function can be used to find cameras geographically. Some cameras/views included in the platform are not shown on this map and must be opened by navigating through the site groups.
7.  **Stream functions bar**
Contains three functions:
reload Individual video stream
Email video snapshot
Capture video snapshot
8.  **View options**
Allows the user to choose how many cameras are displayed on the screen.

Streams Functions Bar

The functions bar contains three functions, as listed below. Notably users can take a snapshot of any stream. The snapshot can then be emailed to a number of recipients (including the user's email), or simply downloaded to the user's device.

Clicking the **Reload Stream** button will reload the individual associated stream. Use this function if there are any streaming issues with the camera feed.



Clicking the **Capture Video Snapshot** downloads a JPG image of the stream onto the user's device.



Clicking the **Email Video Snapshot** button captures a snapshot of the stream and opens a pop-up menu for the user to input details needed for emailing.



When clicking **Email Video Snapshot** a pop-up menu will appear for the user to enter the email addresses of the recipients, a message to go along with the snapshot, and to select whether or not they want the email sent to themselves.

Upon clicking Send, emails will be sent out to all recipients with the snapshot, attached message, and the user who sent the snapshot as seen below.

s9(2)(b)(ii)

vGRID ANPR Overview

What is ANPR?

ANPR stands for **A**utomatic **N**umber **P**late **R**ecognition. ANPR data is produced by a CCTV camera (or system) that can analyse video to capture a vehicle registration plate.

vGRID ANPR

vGRID ANPR has several functions, primarily acting as a database and alerts interface. It provides Police with real-time alerts when stolen vehicles are detected at ANPR sites throughout the country, the ability to lawfully track vehicles and enables users to search a database of all ANPR reads.

vGRID connects to over s9(2)(b)(i) ANPR cameras nationwide that are owned and operated by private business's, business associations, councils, and other entities. SaferCities do not own or operate any ANPR cameras.

vGRID ANPR provides significant benefits in scenarios such as, searching for a suspect's plate during a major investigation like a homicide, or proactively during a firearms incident.

Privacy & Policy

SaferCities and Police comply with the Privacy Act 2020 requirements by adhering to strict internal policies and procedures.

Police have provided SaferCities with their recent ANPR Policy, which outlines the constraints and authority levels for searching the vGRID ANPR database, enabling Police to comply with their policy and legislative requirements. Any misuse of the platform may constitute a breach of Police policy and of the Privacy Act 2020.

NZ Police ANPR policy: <https://www.police.govt.nz/sites/default/files/publications/automatic-number-plate-recognition-140224.pdf>

You must not classify a vehicle as stolen in NIA if the only purpose is to track that vehicle and it has not been stolen.

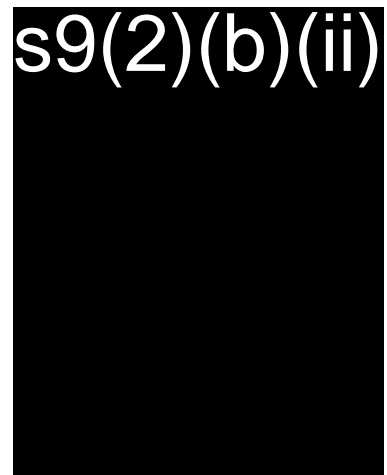
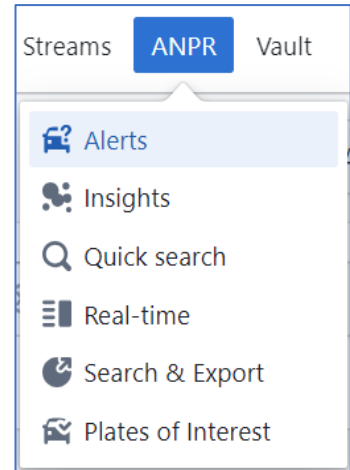
Alerts

The vGRID Alerts function allows users to receive real-time stolen vehicle/stolen plate alerts. The Alerts dashboard enables users to review alerts as they come in and search for existing ones including **Plates of Interest** alerts for tracked vehicles.

Users can search the Alerts dashboard using the search bar and results can be filtered by plate group.

There are two ways to view alerts in detail:

- Once a user receives an alert notification as pictured, they can click on the red popup to go to the specific alert view.
- Alerts can be viewed by clicking on the individual lines as pictured below. This will take users to the specific alert view.



Note: **Not all ANPR cameras are 100% accurate** so you will need you to verify the validity of the data with the associated image. The color of the line next to the plate number indicates if the read is correct, the line will be uncolored if the accuracy of the alert has not been reviewed.

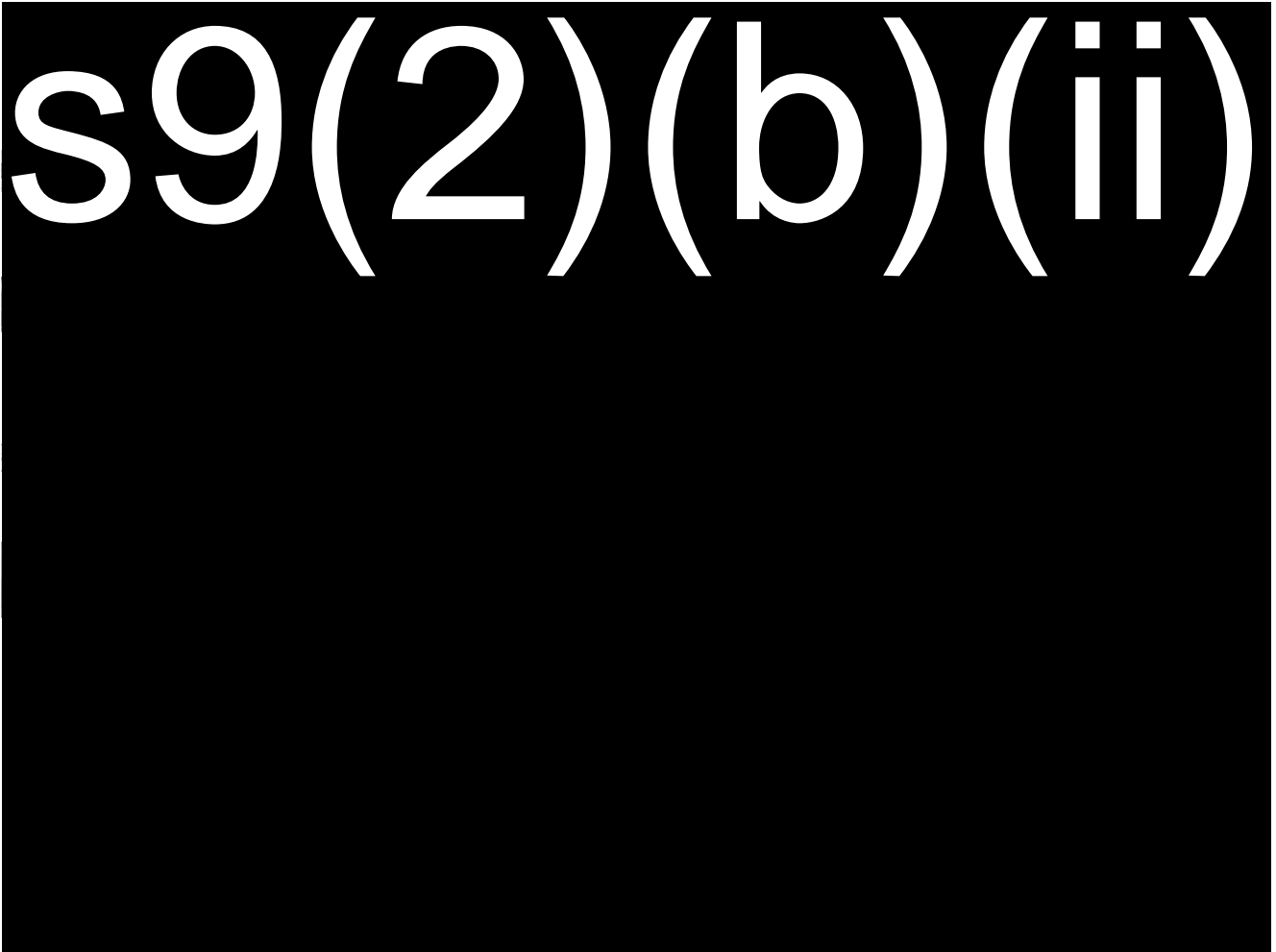
vGRID > ANPR > Alerts List Alert notification settings


Q Search by plate (minimum 3 characters) Notified Alerts ? All Plates

Plate	Camera	Time	Type	
ABC123	49 Main Highway SaferCities Auckland Office ANPR	53 minutes, 11 seconds 01/05/2024 @ 07:51:26	COMMERCIAL VEHICLE	0
ABC124	49 Main Highway SaferCities Auckland Office ANPR	14 hours, 20 minutes 30/04/2024 @ 18:24:23	Station Wagon	0
ABC125	49 Main Highway SaferCities Auckland Office ANPR	17 hours, 10 minutes 30/04/2024 @ 15:34:19	Station Wagon	0
ABC126	49 Main Highway SaferCities Auckland Office ANPR	17 hours, 44 minutes 30/04/2024 @ 15:00:39	CAR	0
ABC126	49 Main Highway SaferCities Auckland Office ANPR	18 hours, 27 minutes 30/04/2024 @ 14:17:11		0
ABC127	49 Main Highway SaferCities Auckland Office ANPR	19 hours, 20 minutes 30/04/2024 @ 13:24:28		0
ABC128	49 Main Highway SaferCities Auckland Office ANPR	23 hours, 45 minutes 30/04/2024 @ 08:59:09	Station Wagon	0

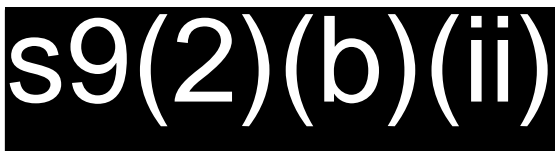
Alert View


View specific alerts and associated details.




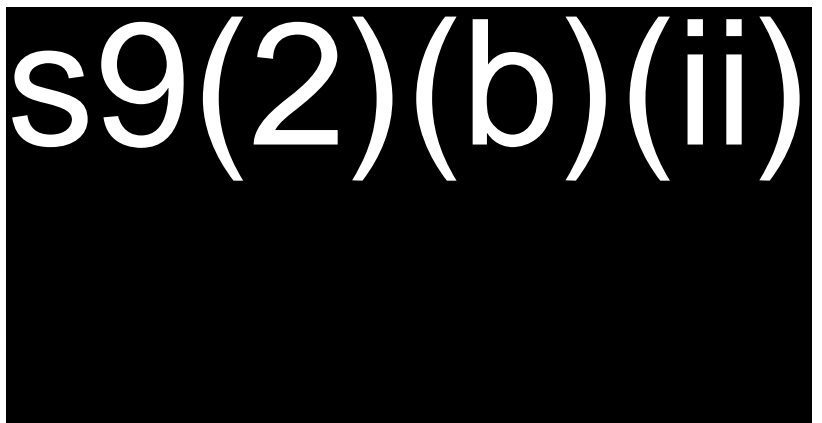
1.  **ANPR read**
A read is returned after the reference image is analysed by an algorithm.

2.  **Reference image**
A cropped image highlighting the registration plate so it can be reviewed.



4.  **Camera location**
ANPR site location icon, used to provide a quick locational overview of the camera.

5.  **ANPR read verification**
Used to manually verify if the ANPR read is correct after reviewing the reference image.



Alert Notifications

Automatic alerts are sent out and displayed when an incoming number plate matches the stolen plate or stolen vehicle list in the Police NIA database. Additionally, any vehicles tracked through the Plate of Interest function.

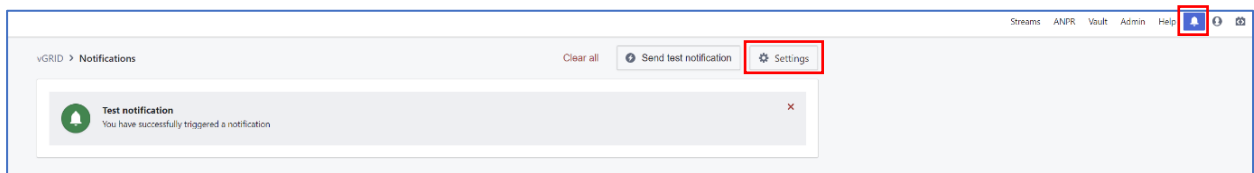
An audible alert sounds if notifications are enabled.

Notification behavior can be altered by changing settings in the Notification settings section.



The Notification settings can be accessed by first going into the Notifications page.

From the Notifications page the settings can be accessed by selecting the Settings button.



These settings enable users to mute sounds for all alerts, to set specific sites of interest that they would like to receive alerts from, or to disable pop ups all together.

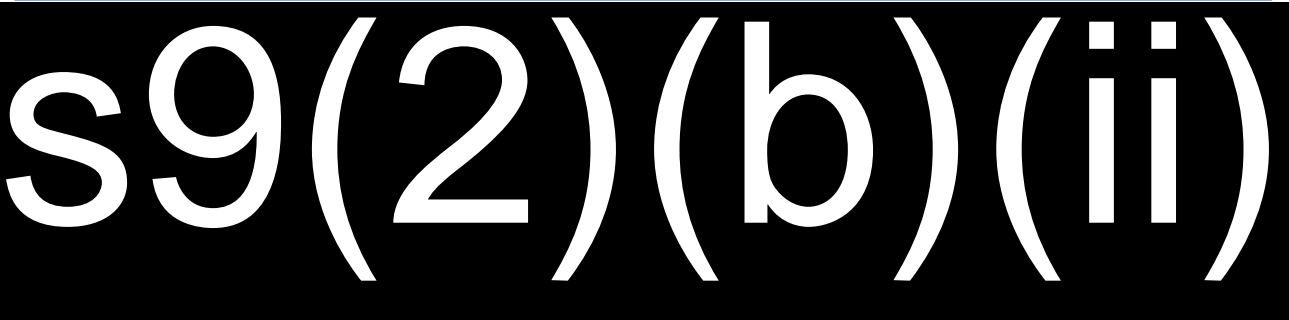
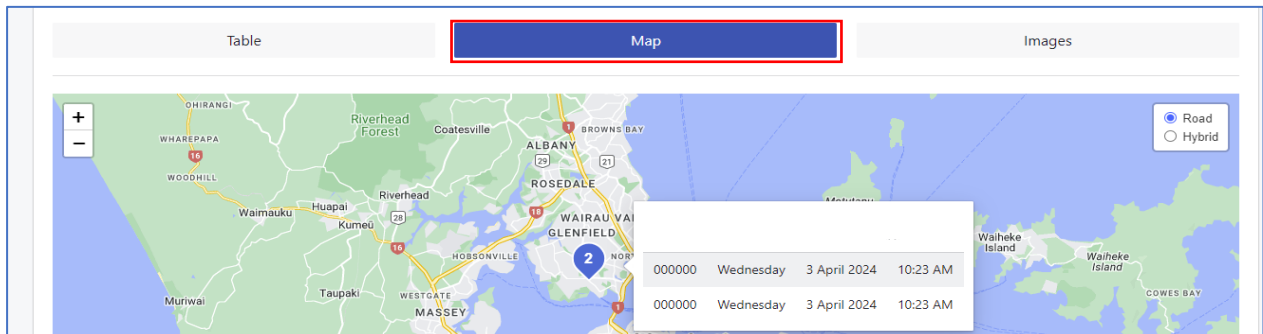
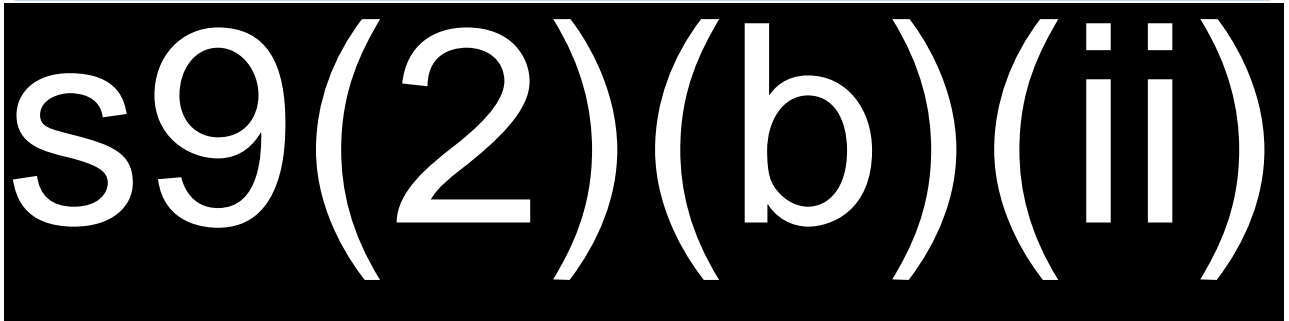
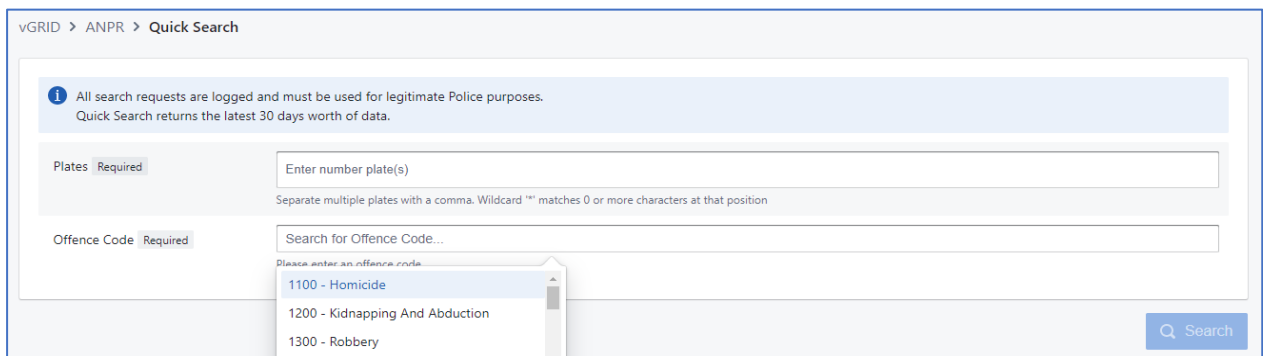
s9(2)(b)(ii)

Quick Search

Quick search enables users to search for ANPR reads within the last **30 days**.

Results can be displayed in one of three views, Table view, Map view and Image view.

Note: a **partial plate search** is possible using '*' in place of up to 3 unknown characters. This will return results ranging from just containing the 3 known characters, up to full 6-character plates. An example is searching ABC*** and the search returning plates such as ABC, ABC5, ABC123, and ABC124.



Search & Export

Search & Export enables users to search for ANPR reads within the last **6 months**.

Entering a number plate and date/time will conduct a search, presenting a preview of results. To view the results, you must get approval by a Senior Sergeant or above. The approver does not have to be a vGRID user.

vGRID > ANPR > Search

Search Parameters Results Preview Request Details Request Sent Request Approved Search Results Ready

i Fill out the form below to preview search results.
 If results are found, you can request approval to view the complete search results.
 Approval should only be requested from someone ranked Senior Sergeant or above.
 All search requests are logged.

Plates **Required**
Separate multiple plates with a comma. Partial plate search is not available.

Start **Required**
Start of search period

End **Required**
End of search period

[Preview results](#)

vGRID > ANPR > Search

Search Parameters Results Preview Request Details Request Sent Request Approved Search Results Ready

i We found 10 results for your search.
 Fill out the remaining fields below to request access to the complete search results.
 Police policy requires your request be approved by someone ranked Senior Sergeant or above, or by a system administrator.
 All search requests are logged.

Plate

Start

End

Case / Event **Required**

Description **Required**
Description of event

Approver **Required**
Email address of the person who will approve your request.
 I approve my own request. My rank is Senior Sergeant or above, or I am a system administrator.

[← New search](#) [Request approval](#)

Once your ANPR export request has been approved, you will receive an email with a link to your results, as well receiving a notification in vGRID.

Your results will be contained in a .zip file. This will include a spreadsheet that contains the date, time, site, camera, and reference to the exported image for each result.

The .zip file also includes cropped images of the number plate as well as the full image of the vehicle for each result.

vGRID > Vault > ANPR Search Results Event log

Search Parameters
Results Preview
Request Details
Request Sent
Request Approved
Search Results Ready

Search details

User: SaferCities Demo (demo@safercities.com)

Case / Event: 000000/0000

Description: Example

Plate: 000000

Search period: 18 March 2024 - 12:00 AM to 17 April 2024 - 3:29 PM

Approved by: demo@safercities.com

Files

Filename	Size	Upload time	Status
anpr-search_2024-03-18-00-00-00_2024-04-17-15-29-45_000000.zip <small>sha256: f6c1bd204e5a39a62afd5e23c2c936d90e6417ce5d1b126d3f6d04e98b915b9</small>	4.25 MB	17 April 2024 - 3:33 PM	Download



A	B	C	D	E	F	G
Id	Plate	Date	Site	Camera	Image	Cropped
1	000000	0000-00-00-00:00:00	Safer Cities	Main Highway	1.jpg	1-cropped.jpg
2	000000	0000-00-00-00:00:00	Safer Cities	Main Highway	2.jpg	2-cropped.jpg
3	000000	0000-00-00-00:00:00	Safer Cities	Main Highway	3.jpg	3-cropped.jpg
4	000000	0000-00-00-00:00:00	Safer Cities	Main Highway	4.jpg	4-cropped.jpg
5	000000	0000-00-00-00:00:00	Safer Cities	Main Highway	5.jpg	5-cropped.jpg
6	000000	0000-00-00-00:00:00	Safer Cities	Main Highway	6.jpg	6-cropped.jpg
7	000000	0000-00-00-00:00:00	Safer Cities	Main Highway	7.jpg	7-cropped.jpg
8	000000	0000-00-00-00:00:00	Safer Cities	Main Highway	8.jpg	8-cropped.jpg
9	000000	0000-00-00-00:00:00	Safer Cities	Main Highway	9.jpg	9-cropped.jpg
10	000000	0000-00-00-00:00:00	Safer Cities	Main Highway	10.jpg	10-cropped.jpg

Plates Of Interest

The primary function of Plates of Interest is to allow Police to **track number plates** using a warrant or relevant warrantless powers. Plates added to these lists will be actively tracked on vGRID, alerting relevant users whenever a plate of interest is detected.

Plates of Interest also provides an overview of all plates you are tracking, as well as all stolen vehicle/plates. You can select the drop-down box to filter the plate group you require.

To track a plate select **Add Plate of interest**. Then fill out the required details shown below.

vGRID > ANPR > Plates of Interest ➕ Add Plate of Interest

vGRID ANPR Plates of Interest
 This feature allows you to enter a vehicle plate of interest for active detection and alerting against ANPR reads connected to the vGRID SaferCity Platform. Your ability to use this feature within the vGRID SaferCity platform mandates compliance with legislation.

🔍 Search by plate (minimum 3 characters) All Plates ▾

Plate	Type	Make	Model	District	Start
ABC123	CAR	NISSAN	LUCINO	AUCKLAND CITY	01/05/23 @ 09:16
...	01/05/23

vGRID ANPR Plates of Interest
 This feature allows you to enter a vehicle plate of interest for active detection and alerting against ANPR reads connected to the vGRID SaferCity Platform. Your ability to use this feature within the vGRID SaferCity platform mandates compliance with legislation.

As per NZ Police's ANPR Policy (draft), tracking may only be used with the appropriate authority:

- Under a Tracking Warrant
- Under Section 48 of the Search & Surveillance Act
- Where there is a need to prevent or lessen a serious threat to someone's life or a serious threat to public health or public safety, but no offence is suspected.

Plate of Interest Required

Tracking period Required
 17 April 2024 - 1:55 PM 📅
Start time (required) End time (optional)

Plates of Interest Group Required
 My Plates of Interest ▾
Which group this plate should be added to

Police File / Event # Required

Authoriser Email Required

Reason For Tracking Required
 Select a reason ▾
Please select a reason for tracking

Offence Code Required

Please enter an offence code

Notes Required

⌵ Optional Details

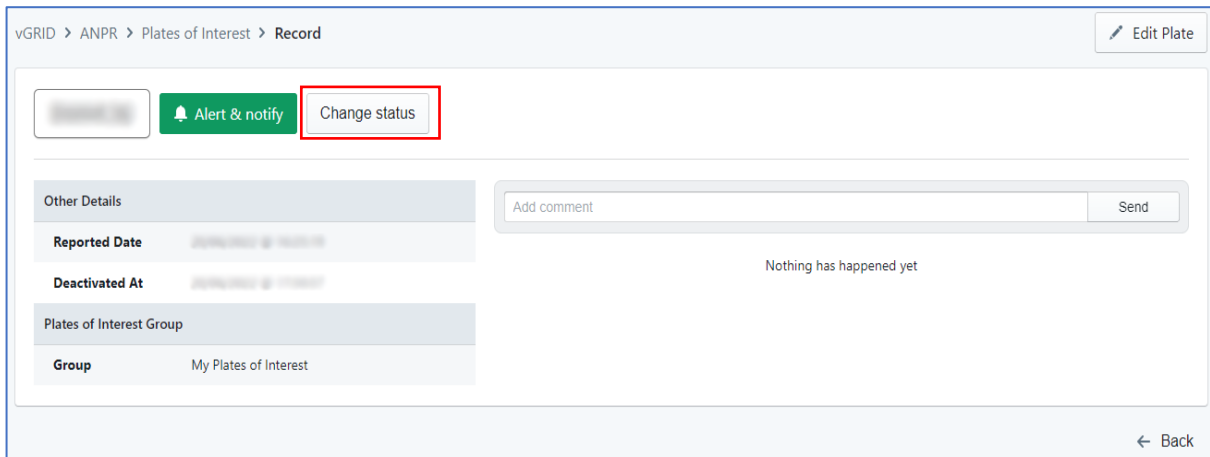
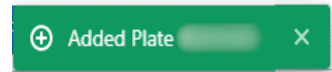
⚠️ I confirm that I have correctly followed any internal policy and have the necessary authority or warrant to undertake a lawful search.
 If required, I will provide a relevant warrant as soon as practicable and am aware that my searches may be audited.
Where relevant you must enter in the correct date and time period for tracking.
 SaferCities accepts no responsibility for plates added without permission.

I Agree

← Back Create

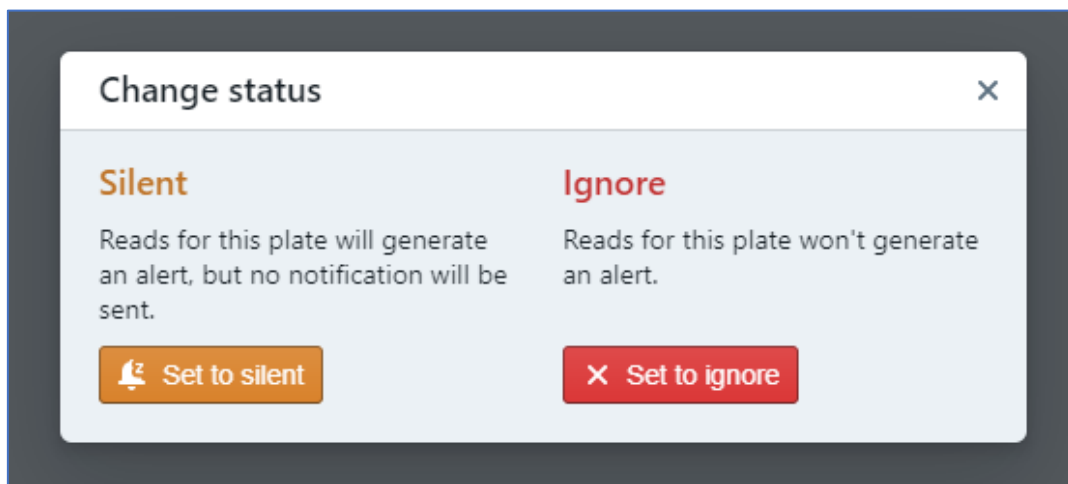
Optional details such as vehicle type, model, colour etc can also be set in the optional details drop-down section.

After entering the relevant information, accepting the agreement, and clicking create, a pop-up will appear to confirm the plate has been added. The Record page will then be loaded.



The **Record** page will show the specific plate of interest, with its relevant information, attached comments, status, and settings. Here comments can be made or viewed and the plates original setup page can be reopened for editing.

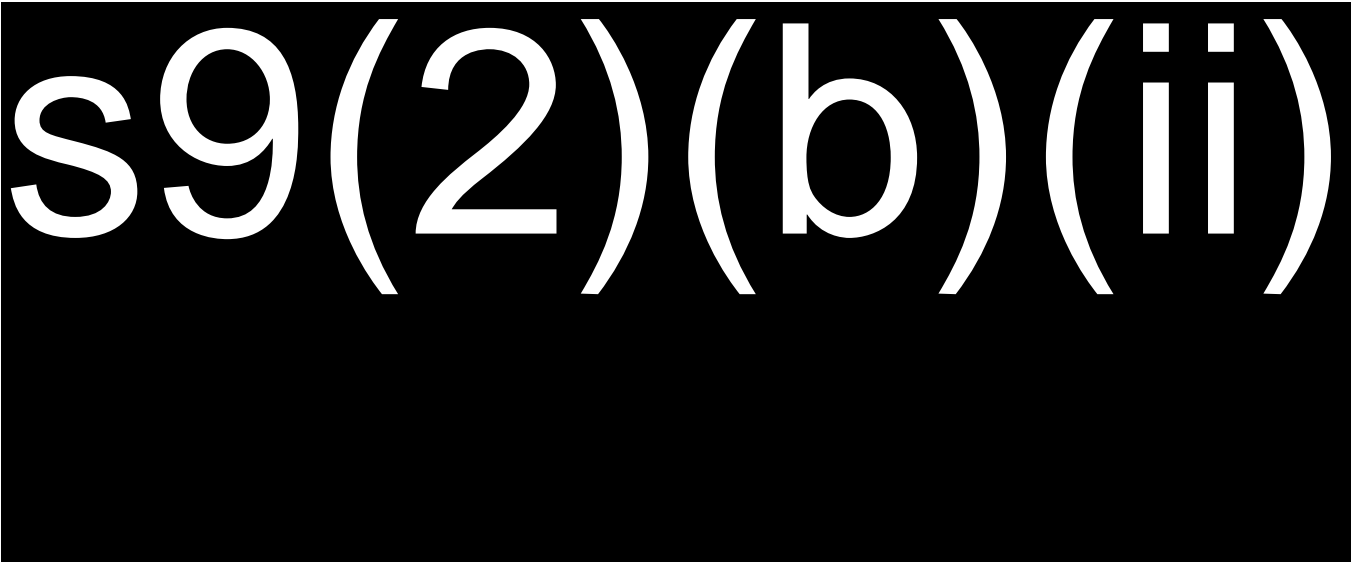
The settings around notifications and alerts can also be changed on the Record page. This is done by selecting change status. The status can be set to Silent or Ignore which configures the alerts to not notify users, or not alert at all.



Insights

Allows users to view a heatmap and statistics relating to vGRID ANPR including the number of reads and alerts.

This function is restricted to specialist users.



Realtime

Allows users to see ANPR plate reads in real time.

vGRID > ANPR > Real-time

Plate	Camera	Time
ABC123	49 Main Highway SaferCities Auckland Office ANPR	9:05 AM 1 May 2024
ABC124	49 Main Highway SaferCities Auckland Office ANPR	9:04 AM 1 May 2024
ABC123	49 Main Highway SaferCities Auckland Office ANPR	9:04 AM 1 May 2024
ABC124	49 Main Highway SaferCities Auckland Office ANPR	9:04 AM 1 May 2024
ABC123	49 Main Highway SaferCities Auckland Office ANPR	9:04 AM 1 May 2024
ABC124	49 Main Highway SaferCities Auckland Office ANPR	9:04 AM 1 May 2024
ABC123	49 Main Highway SaferCities Auckland Office ANPR	9:04 AM 1 May 2024
ABC124	49 Main Highway SaferCities Auckland Office ANPR	9:04 AM 1 May 2024

vGRID Vault Overview

Vault is an easy way for Police to request and obtain digital evidence from a member of the public without the need for a physical visit. After a request has been completed, relevant files arrive straight to you, accompanied by a report to preserve the chain of custody.

Files transferred to Vault are **only retained for 30 days**.

An unlimited number of files may be uploaded. However, there is a per-file size limit of 4GB. All files are also 'hashed' to prevent tampering of evidence. Hashing ensures that files uploaded by the member of public remains unchanged throughout the chain of custody.

Vault is not intended as a replacement for secure local Police file storage, NIA or IMT.

CCTV footage and images obtained through Vault should be stored appropriately within Police.

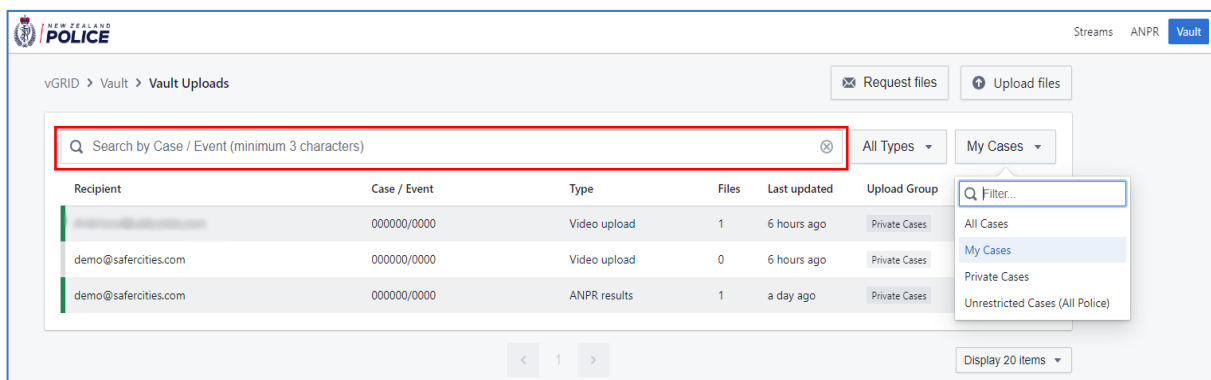
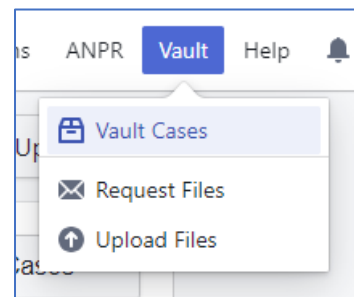
vGRID Vault Cases Dashboard

The Vault cases dashboard contains a list of your cases. This can be filtered to show all public cases (Internal Police requests).

You can also search for relevant details like case number using the search bar.

Request files: Request files from people outside of your organisation.

Upload files: Share files internally with your organisation.



vGRID Vault Request Files

After clicking the request file button, fill out the required details to complete your request.

Choose your desired upload group:

Private (Default): Only visible to you or the person you assign as the owner.

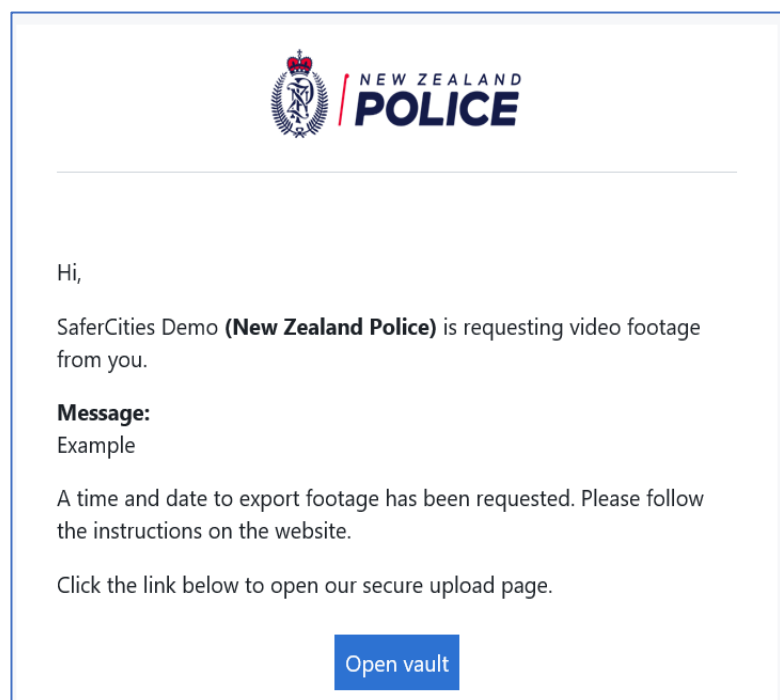
Unrestricted: visible to your organisation.

The screenshot shows a 'Request files' form with the following fields and values:

- Email address (Recipient of Vault request):** demo@safercities.com
- Case / Event:** 000000/0000
- Start:** 17 April 2024 - 9:17 AM
- End:** 17 April 2024 - 9:18 AM
- Message:** Example
- Upload group:** Private Cases (highlighted with a red box)

At the bottom, there is a search filter for upload groups, showing 'Private Cases' and 'Unrestricted Cases (All Police)'. A 'Send request email' button is located at the bottom right.

Once you select send request an email containing a link and instructions on how to upload files will then be sent to the recipient.



A chain of custody PDF can be generated at any time using the **Generate PDF** button.

You will be notified when files are uploaded to your Vault case. Once you are satisfied with the files and want to close the Vault request, you can select complete. The case will remain visible to you.

Using the edit button allows you to change the case owner and any relevant details

Filename	Size	Upload Time
screenshot-2024-04-18-153554.png sha256: 4c4735d3dc244a0bef8cff14c71d220bf676ec6afeef5cbe32c8170f3d0d7944	59.8 kB	22/04/2024 08:50:14

vGRID Vault Upload Files

The Upload files option allows members of the Police to upload and share files internally, in a similar manner to that of the Request files function.

Leaving the “**I need receipt details**” button unticked enables a file to be uploaded without recipient details.

If set to public, the file can then be shared to internal staff using the URL (Link) or found by searching vault cases.

VGRID

SaferCity Platform

Police Lite User Guide

7 May 2024 – v3.0



Table of Contents

vGRID SaferCity Platform Overview	2
Requesting access to vGRID	3
Support for vGRID	3
How to access vGRID via a Police Enterprise PC.....	3
vGRID Vault Overview	4
Vault Cases Dashboard.....	4
Vault Request Files	5
Vault Upload Files	7

vGRID SaferCity Platform Overview

The vGRID SaferCity Platform is software for Police. It provides access to live and historical information. This includes live CCTV cameras, operator screens, and vehicle number plate reads (ANPR).

The platform also includes vGRID Vault, providing Police with the ability to request digital files from victims and witnesses. Members of the public can then be sent a link which allows them to upload evidence (video, images, or other), allowing the Police to receive evidence digitally without a physical visit.

This guide is designed for use on Desktop/Laptop devices. Not all of the functions highlighted below are available for mobile users.



Respond

Investigate

STREAMS
Live video

CCTV Cameras
Specialist screens

ANPR
Database

Live alerts
Historic search

Vault
Evidence request

Request digital files
from the public

Requesting access to vGRID

If you are unable to log into vGRID using your NZ Police email and password or to request additional permissions, please email our support inbox with the following details:

- 'Access to vGRID' in the email title
- Physical location
- Workgroup
- Reason for access

Support for the vGRID Platform

For any vGRID related enquiries, please visit our online user guide and FAQ's using the links below. Alternatively, contact us via phone or email using the details provided.

F.A.Q - docs.vgrid.io/faq

Email - support@safercities.com

Phone - 09 281 9777

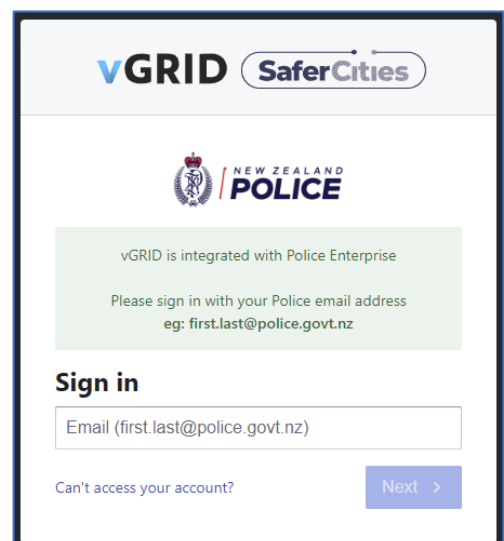
How to access vGRID via a Police Enterprise PC

1. Using a NZ Police computer, open vGRID using the linked provided:

- **s.6(c) OIA**

2. Log in using:

- `firstname.lastname@police.govt.nz`
- Your Police Enterprise password



vGRID Vault Overview

Vault is an easy way for Police to request and obtain digital evidence from a member of the public without the need for a physical visit. After a request has been completed, relevant files arrive straight to you, accompanied by a report to preserve the chain of custody.

Files transferred to Vault are **only retained for 30 days**.

An unlimited number of files may be uploaded. However, there is a per-file size limit of 4GB. All files are also 'hashed' to prevent tampering of evidence. Hashing ensures that files uploaded by the member of public remains unchanged throughout the chain of custody.

Vault is not intended as a replacement for secure local Police file storage, NIA or IMT.

CCTV footage and images obtained through Vault should be stored appropriately within Police.

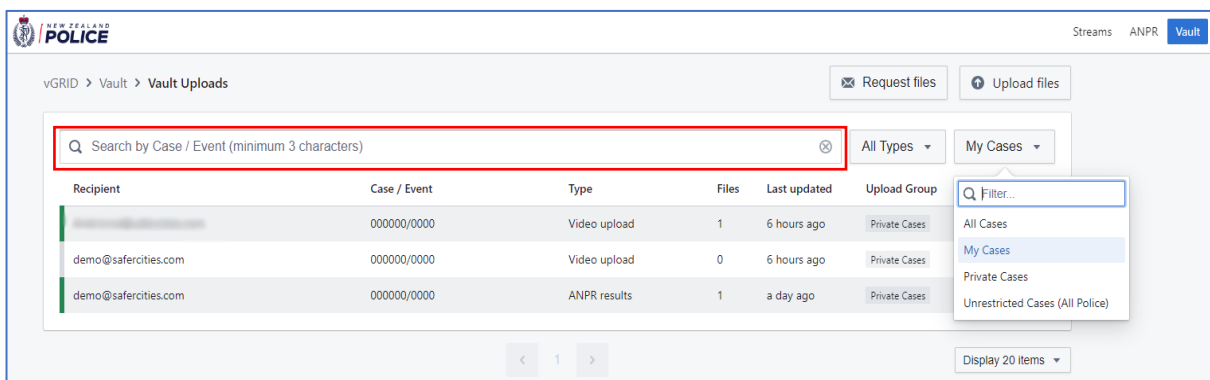
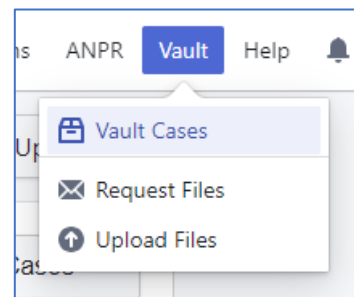
vGRID Vault Cases Dashboard

The Vault cases dashboard contains a list of your cases. This can be filtered to show all public cases (Internal Police requests).

You can also search for relevant details like case number using the search bar.

Request files: Request files from people outside of your organisation.

Upload files: Share files internally with your organisation.



vGRID Vault Request Files

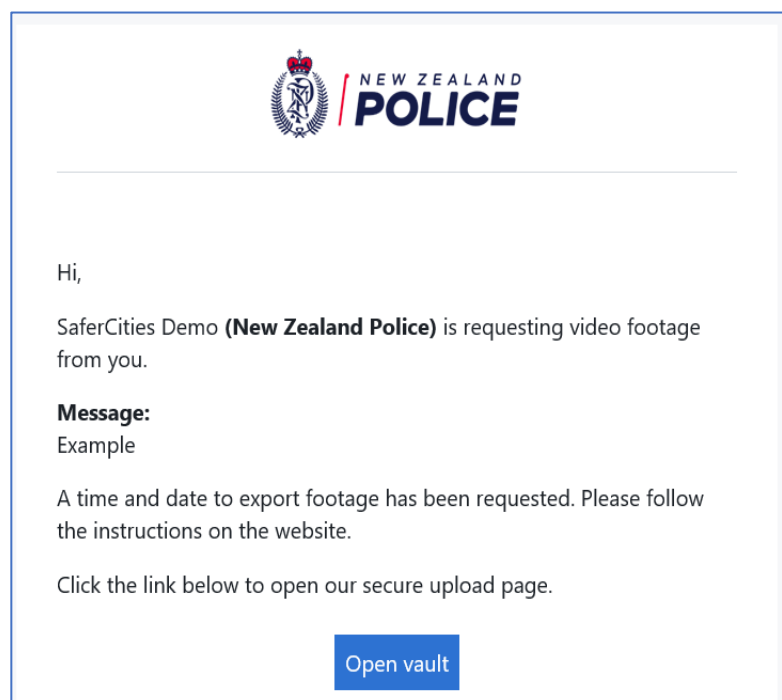
After clicking the request file button, fill out the required details to complete your request.

Choose your desired upload group:

Private (Default): Only visible to you or the person you assign as the owner.

Unrestricted: visible to your organisation.

Once you select send request an email containing a link and instructions on how to upload files will then be sent to the recipient.



A chain of custody PDF can be generated at any time using the **Generate PDF** button.

You will be notified when files are uploaded to your Vault case. Once you are satisfied with the files and want to close the Vault request, you can select complete. The case will remain visible to you.

Using the edit button allows you to change the case owner and any relevant details

Filename	Size	Upload Time
screenshot-2024-04-18-153554.png sha256: 4c4735d3dc244a0bef8cff14c71d220bf676ec6afeef5cbe32c8170f3d0d7944	59.8 kB	22/04/2024 08:50:14

vGRID Vault Upload Files

The Upload files option allows members of the Police to upload and share files internally, in a similar manner to that of the Request files function.

Leaving the “**I need receipt details**” button unticked enables a file to be uploaded without recipient details.

If set to public, the file can then be shared to internal staff using the URL (Link) or found by searching vault cases.

vGRID > Vault > Upload

Create Request
Request Sent
Request Opened
Request Completed

Case / Event Required: 000000/0000

Case owner Required: SaferCities Demo (demo@safercities.com)

Message: Example

Upload group Required: Unrestricted Cases (All Police)

Time period: 21 April 2024 - 9:08 AM to 22 April 2024 - 9:08 AM

Time difference: Days: 0, Hours: 0, Minutes: 0, Seconds: 0, Direction: None

I need recipient details

Filename	Size	Upload time	Status
screenshot-2024-04-22-085037.png sha256: unknown	64.85 kB	22 April 2024 - 9:07 AM	In Queue

Drag files here to upload, or click the Add file button

Add file

← Back Upload Files and Complete

s.6(c) OIA

vGRID > Vault > Upload

Event log Generate PDF

Create Request
Request Sent
Request Opened
Request Completed

Request information

Case / Event: 000000/0000

Case owner: SaferCities Demo

Upload group: Unrestricted Cases (All Police)

Privacy Policy - vGRID SaferCity Platform

Please read our privacy policy. It is important, and we have tried to make it simple and straight up. This Policy was last updated on **6 July 2024** and is for New Zealand.

For the Privacy Policy of the vgrid.io website please visit vgrid.io/privacy/website

Our work

Safer City Group Limited (trading as SaferCities) provides the vGRID SaferCity Platform for Users to access CCTV networks efficiently and lawfully.



CCTV

Owned and operated by local agencies



vGRID

Enables effective and controlled sharing with Users



Users - like Police

Can lawfully access footage and fight crime

CCTV networks are owned and operated by agencies like your local city council, local shops, supermarkets, drive-throughs and retailers.

Traditionally, when something went wrong - a theft, a ram raid, a stolen vehicle - these CCTV networks were hard for Users like the New Zealand Police to access.

vGRID makes it easier for Users to access those networks efficiently to detect, investigate and prevent crime in your neighborhood through our platform.

You can think of this like a pipeline - we link information between two groups, for the benefit of everybody. We don't use personal information on the platform for our own purposes, we process information on behalf of CCTV operators, and the Users of the platform.

vGRID SaferCity Platform

vGRID promotes the philosophy that more effective and efficient policing occurs when the community and Users can communicate effectively. Users can request access to a CCTV camera (or camera system), and then receive live footage. Information is securely transmitted between the two parties through the vGRID SaferCity Platform. Users can see what is happening in real time but are unable to record the footage at their end.

vGRID ANPR

vGRID ANPR (Automatic Number Plate Recognition) receives number plate records created by CCTV operators' systems and compares it against stolen and other warranted 'Plates of Interest' lists. Where a match occurs, Users are alerted. Personal information is limited - Users receive from the camera the vehicle number plate, date and time and location of the image capture, and a still image of the capture from the camera. This will only happen when a car is registered as stolen and when the Police use the system lawfully.

vGRID Vault

vGRID Vault makes it easier for CCTV operators and the Users to interact. It is built to ensure Users meet their chain of evidence requirements, and with strict

Users send a request through the platform, which then prompts the CCTV operators to upload the desired footage or related evidence, alongside some basic information about the individual uploading the information (Name, Date of Birth, Contact Information).

Our commitment to you as a data guardian

We care about your community, and your privacy.

SaferCities is a community focused organisation: we want safe and vibrant cities for Aotearoa New Zealand. We know that CCTV is a complex topic, and our platform improves CCTV for everyone involved because it helps ensure CCTV is fit for purpose and increases its effectiveness.

As part of our commitment to the community, we take privacy very seriously. Our platform is designed to minimise the amount of personal information involved.

Fundamentally, it is a pipeline between the CCTV operators and the Users of our platform. We have several inbuilt safeguards so that User access is recorded, and we have strict contracts in place with all parties.

We are data guardians.

We keep information safe and secure, both at our premises and within our platform.

We believe strongly in data-sovereignty and the importance of keeping things local. Our primary servers are hosted in New Zealand, and we use Amazon AWS in Australia to store Vault and ANPR footage/images. We have ensured we are following industry standard encryption and security protocols including zero-trust cloud infrastructure.

When Users access vGRID, this requires strict permissions and Users must meet identity management standards.

Internally, we have a small team who know each other well and work closely: our access is restricted solely to our technicians, and we all abide by an internal suite of policies and processes to ensure we only access the platform for legitimate reasons, examples of which are maintaining the platform, completing troubleshooting, and facilitating the platform functions that Users access.

We'll help you wherever we can.

correct any information if it is wrong. This will apply if there is something that identifies you.

If you have concerns with a CCTV operator, want to exercise any of your rights under the Privacy Act 2020, or want some help to exercise your rights, we will always do our best to facilitate the best outcome for everybody.

If you have any concerns, want to talk to us, or want help with your privacy rights, please contact us at privacy@safercities.com



Legal

[Product Warranty](#)

[Terms of Use](#)

[Terms of Trade](#)

Privacy

[Policy - Website](#)

[Policy - Platform](#)

[Policy - Mobile App](#)

SaferCities ANPR (previously known as VGRID ANPR)

Brief Privacy Analysis

26th February 2021 (updated 25th July 2024)

1. Project summary: VGRID ANPR SaferCities

1.1 Brief description of the project

The vGRID ANPR module from SaferCities is a software module within the larger vGRID SaferCity Platform for Police and private organisations that receives various formats of Automatic Number Plate Records (ANPR) generated by the different CCTV systems held by each organisation, compares them to a continuously updated list of number plates of stolen vehicles and stolen number plates themselves, and where a match occurs, creates an alert to Police in near real-time.

When activated by police staff, this alert contains a link to the Number Plate Information (NPI) which consists of the number plate text, description of vehicle, date, time and location of capture and associated images of the cropped plate and the image it is derived from if it is available. Any previous comments made by police relating to this NPI are also displayed within the VGRID ANPR alert screen. Police then decide what action to take.

ANPR technology is used to help detect, deter and disrupt criminality and is used globally. vGRID ANPR connects those businesses and organisations who wish to share with Police their ANPR information, (captured by whichever camera and software system they use) via a SaferCities data processing service. This service in real-time processes that data with publicly available stolen vehicle/plate information provided by Police and if a match occurs sends details (NPI) of that match to police as an alert.

The main stakeholders involved are the public, businesses and organisations who have opted into this service and the Police.

1.2 Personal information that the project will involve

The Privacy Act 2020 defines “Personal information” as any information about an identifiable living person. However, a person doesn’t have to be named in the information to be identifiable. The vGRID ANPR module involves comparing of number plates from images of vehicles captured in public places through use of an optical character recognition software to recreate the alphanumeric characters of the vehicles number plate in a format which can be compared with a police generated list of stolen plates or vehicles. Guidance from the Office of the Privacy Commissioner states, “that a car’s number plate would not be personal information on its own - all you know from a number plate is the number itself, and the make and model of the car it’s attached to.” Since there is no information referring to the owner’s name, address or other personal information within the vGRID ANPR SaferCities domain, this project does not involve personal information. Subsequent matching of ANPR alerts with vehicle registration and other databases which would include personal information, occurs within the Police environment.

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 <i>Example: New legislation or policy that makes it compulsory to collect or disclose information</i>		N	
Any practice or activity that is listed on a risk register kept by your organisation <i>Example: Practices or activities listed on your office's privacy risk register or health and safety register</i>		N	
Collection			
A new collection of personal information <i>Example: Collecting information about individuals' location</i>		N	
A new way of collecting personal information <i>Example: Collecting information online rather than on paper forms</i>		N	
Storage, security and retention			
A change in the way personal information is stored or secured <i>Example: Storing information in the cloud</i>		N	

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

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 <i>Example: A phone company adopts a new policy of searching data in old phones that are handed in</i>		N	
Surveillance, tracking or monitoring of movements, behaviour or communications <i>Example: Installing a new CCTV system</i>	Y		3rd Party CCTV systems are used in public places to create ANPR capture and associated Number Plate Information. However, no matching with other databases is done within VGRID ANPR to create personal information.
Changes to your premises that will involve private spaces where clients or customers may disclose their personal information <i>Example: Changing the location of the reception desk, where people may discuss personal details</i>		N	
New regulatory requirements that could lead to compliance action against individuals on the basis of information about them <i>Example: Adding a new medical condition to the requirements of a pilot's license</i>		N	
List anything else that may impact on privacy, such as bodily searches, or intrusions into physical space		N	

2.2 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.

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).

If you answered “No” to all the questions in 2.1 above, move on to section 3 below.

Aspect of the Project	Rating (L, M or H)	Describe any medium and high risks and how to mitigate them
<p>Level of information handling</p> <p>L – Minimal personal information will be handled</p> <p>M – A moderate amount of personal information (or information that could become personal information) will be handled</p> <p>H – A significant amount of personal information (or information that could become personal information) will be handled</p>	L	
<p>Sensitivity of the information (eg health, financial, race)</p> <p>L – The information will not be sensitive</p> <p>M – The information may be considered to be sensitive</p> <p>H – The information will be highly sensitive</p>	L	
<p>Significance of the changes</p> <p>L – Only minor change to existing functions/activities</p> <p>M – Substantial change to existing functions/activities; or a new initiative</p> <p>H – Major overhaul of existing functions/activities; or a new initiative that’s significantly different</p>	L	

<p>Interaction with others</p> <p>L – No interaction with other agencies</p> <p>M – Interaction with one or two other agencies</p> <p>H – Extensive cross-agency (that is, government) interaction or cross-sectional (non-government and government) interaction</p>	M	<p>Police can enter comments within the VGRID ANPR Alert, once opened, and if personal information is inputted, it is visible to Police users within VGRID ANPR and SaferCities technicians who service the VGRID ANPR SaferCities infrastructure.</p>
<p>Public impact</p> <p>L – Minimal impact on the organisation and clients</p> <p>M – Some impact on clients is likely due to changes to the handling of personal information; or the changes may raise public concern</p> <p>H – High impact on clients and the wider public, and concerns over aspects of project; or negative media is likely</p>	L	

3. Summary of privacy impact

The privacy impact for this project has been assessed as:	Tick
<p>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</p>	X
<p>Medium – Some personal information is involved, but any risks can be mitigated satisfactorily</p>	
<p>High – Sensitive personal information is involved, and several medium to high risks have been identified</p>	
<p>Reduced risk – The project will lessen existing privacy risks</p>	
<p>Inadequate information – More information and analysis is needed to fully assess the privacy impact of the project.</p>	

3.1 Reasons for the privacy impact rating

No personal information is collected, used or stored within VGRID ANPR outside of the Police domain. Police can associate personal information with data obtained from VGRID ANPR SaferCities, but this is done within the Police domain and their obligations to comply with the Privacy Act 2020.

4. Recommendation

A full privacy impact assessment is not required

Project VGRID ANPR SaferCities does not involve the collection of personal information. Any matches of data collected by VGRID ANPR to personal information, such as registered owner details, is undertaken by Police and is outside of the scope of this analysis. If through the course of database upkeep and maintenance, SaferCities staff see a comment containing personal information entered by police on a VGRID ANPR Alert, they will ignore it as per SaferCities Privacy Policy (see Appendix A).

5. Sign off

Scott Bain

Signature

Managing Director SaferCities

____/____/____
Date

Chris Wiggins

Name

Chief Technology Officer

Position (Manager)

Signature

____/____/____
Date

SaferCities Privacy Policy

SaferCities complies with the New Zealand Privacy Act 2020 (the Act) when dealing with personal information. Personal information is any information about an identifiable living person. However, a person does not have to be named in the information to be identifiable and information can become personal information when combined or linked with other information.

All SaferCities staff are required to be familiar with the 13 principles of the Privacy Act 2020 and the Privacy Breach notification process. To achieve this staff are required to undertake the following:

- Office of the Privacy Commissioner's eLearning courses: The Privacy Act 2020, Privacy Breach Reporting, and A Guide to Privacy Impact Assessments. Certificates are obtained upon successful completion of each course.
- Further Privacy Act 2020 compliance training as required.

To ensure the protection of privacy is at the heart of what we do, SaferCities uses the Privacy by Design (PbD) principles and privacy impact assessments (PIA) where appropriate when undertaking projects (see overleaf). These are considered best practice around the world.

Where a project deals with personal information, a specific privacy policy for that project will be created, setting out how we will collect, use, disclose and protect that personal information.

When dealing with 3rd party data, if an actual or potential privacy breach is detected, SaferCities will notify the owning organisation of the potential breach for their remedial action and if no action is taken, consider notification of that breach to the Privacy Commissioner themselves.

Scott Bain

CEO, SaferCities

This Policy was last updated on 26th February 2021 & has been reviewed annually

Next Review due on 1st February 2025

Privacy by Design (PbD)

Seven principles:

1. Proactive not reactive; preventative not remedial. Anticipate privacy risks and mitigate.
2. Privacy as the default setting. Automatically protect personal information. Collect minimum information required and restrict access to information on a “need to know” basis.
3. Privacy embedded into design. Privacy central to core functionality and integrated into all IT systems and business processes.
4. Full functionality – positive-sum, not zero-sum. Possible to have win-win solution protecting privacy and meeting business requirements.
5. End-to-end security – full cycle protection. Apply privacy protections throughout the lifecycle of personal information in any system or process inc storage, access, use and disclosure.
6. Visibility and transparency – keep it open. Publish plain-language policy statements, privacy impact assessments to assure people you have suitable protections in place. Helps build trust with stakeholders.
7. Respect for user privacy. Design solutions with customers in mind. Strong privacy defaults, appropriate notices and user-friendly options, including in operational changes.

Privacy Impact Assessment

Five key steps:

1. Define the purpose of the project and document/map out the information flows.
2. Check that your proposed collection, use and disclosure of personal information complies with the privacy principles.
3. Identify privacy risks and decide how best to avoid or mitigate them.
4. Align privacy analysis with your agency’s existing risk, information and project management methods. Determine the governance arrangements you need to support the initiative and consider any implications for third parties.
5. Produce a report that records the analysis and that can be used for decision-making.

A privacy threshold assessment is a preliminary, high level analysis that lets you see whether you need to undertake a more thorough PIA. It can help you identify and record whether your proposal raises privacy risks, assess those risks, and work out how to mitigate or manage them.

vGRID SaferCity Platform

Live Streaming s9(2)(b)(ii)

Brief Privacy Analysis

1st March 2020

1. Project summary: vGRID SaferCity Platform – Live Streaming

1.1 Brief description of live streaming on the vGRID SaferCity platform

The vGRID SaferCity Platform is live streaming software that provides Police with live visual information on request and when appropriate, in a secure and authenticated way.

Live visual information includes CCTV cameras (nominated cameras only) or CCTV operator screens (screen share). Visual information can be shared 'live' but is not recorded.

The platform promotes the philosophy that more effective and efficient policing and Police deployment results when the community and public can more easily share live visual information that is relevant and appropriate to Police, when they need it.

Sharing of live visual information between the CCTV asset owner (nominated cameras or screens only) and Police is defined within a standard MoU process that complies with the Privacy Act and the Privacy Policy of the CCTV asset owner and Police.

The vGRID SaferCity Platform can also be used to see live streams of cameras or CCTV operator screens from other organisations who agree to share.

vGRID SaferCity Platform has been in use nationally by NZ Police since 2015, is constantly improving and evolving, and is designed collaboratively with both NZ Police and community organisations.

Other stakeholders that help evolve the platform include councils, transportation, private businesses and large organisations who opt in and leverage this live streaming service with the Police.

1.2 Personal information that the project will involve

The Privacy Act 2020 defines “Personal information” as any information about an identifiable living person. However, a person doesn’t have to be named in the information to be identifiable. Guidance from the Office of the Privacy Commissioner “Privacy and CCTV A guide October 2009”, states that “Because CCTV captures images of people, which can be used, stored, manipulated and disseminated, those people who operate the systems need to be aware of how to manage privacy issues.” This refers to the operators of non-covert CCTV in public and semi-public places complying with the privacy principles in the Privacy Act 2020.

SaferCities does not operate CCTV networks, rather it provides the technological solution to share images captured by CCTV operations with the Police or other organisations to better support Police and the prevention and detection of crime and the safety of customers and the public.

Therefore, the primary obligations to comply with the Privacy Act lies with each CCTV operator and the Police, and their CCTV Policy, Privacy Policy and Privacy Impact Assessment should address their obligations under the Privacy Act 2020, as illustrated below:

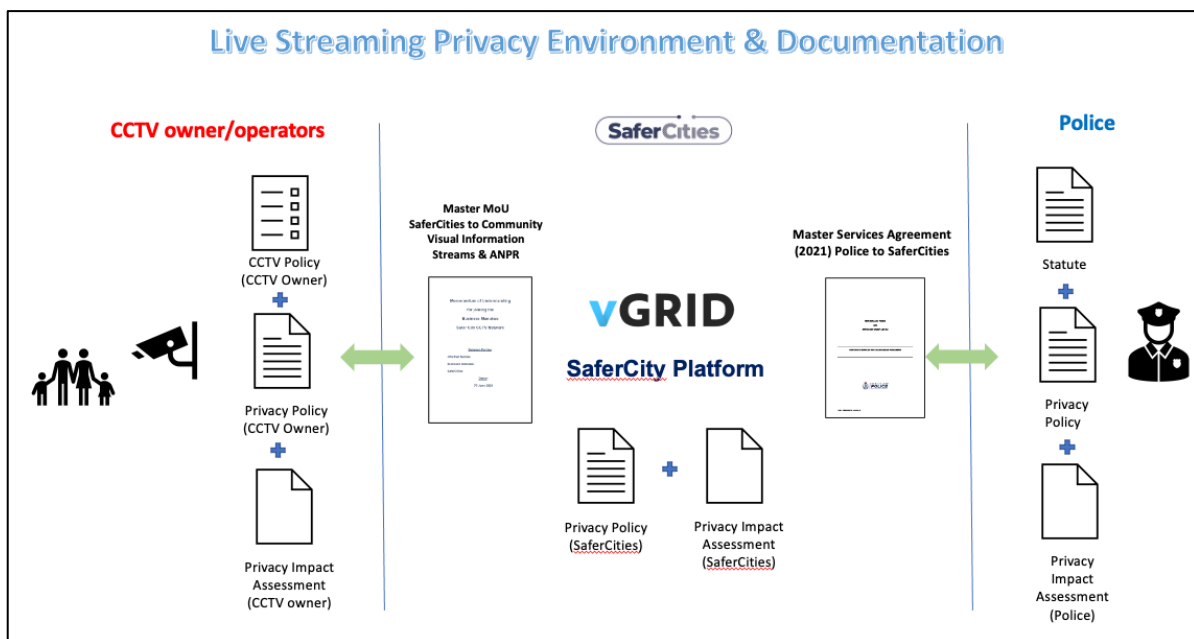


Figure 1: Livestream privacy environment

Link to CCTV guidance: <https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/Privacy-and-CCTV-A-guide-October-2009.pdf>

2. Privacy assessment

2.1 Areas that are risky for privacy

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 <i>Example: New legislation or policy that makes it compulsory to collect or disclose information</i>		N	
Any practice or activity that is listed on a risk register kept by your organisation <i>Example: Practices or activities listed on your office's privacy risk register or health and safety register</i>		Y	Protection of data with respect to cyber security threats. Already addressed through Risk Treatment Plan as part of normal business activity for a technology firm.
Collection			
A new collection of personal information <i>Example: Collecting information about individuals' location</i>		N	
A new way of collecting personal information <i>Example: Collecting information online rather than on paper forms</i>		N	
Storage, security and retention			
A change in the way personal information is stored or secured <i>Example: Storing information in the cloud</i>		N	
A change to how sensitive information is managed <i>Example: Moving health or financial records to a new database</i>		N	
Transferring personal information offshore or using a third-party contractor <i>Example: Outsourcing the payroll function or storing information in the cloud</i>		N	

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

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 <i>Example: A phone company adopts a new policy of searching data in old phones that are handed in</i>		N	
Surveillance, tracking or monitoring of movements, behaviour or communications <i>Example: Installing a new CCTV system</i>	Y		3rd Party CCTV systems are used in public places and the owners of these systems have responsibility to comply with the Privacy Act. The SaferCities Platform provides a secure transmission of livestreams to Police and CCTV operators and complies with Privacy Act requirements for data access and security under its Privacy Policy.
Changes to your premises that will involve private spaces where clients or customers may disclose their personal information <i>Example: Changing the location of the reception desk, where people may discuss personal details</i>		N	
New regulatory requirements that could lead to compliance action against individuals on the basis of information about them <i>Example: Adding a new medical condition to the requirements of a pilot's license</i>		N	
List anything else that may impact on privacy, such as bodily searches, or intrusions into physical space		N	

2.2 Initial risk assessment

Aspect of the Project	Rating (L, M or H)	Describe any medium and high risks and how to mitigate them
<p>Level of information handling</p> <p>L – Minimal personal information will be handled</p> <p>M – A moderate amount of personal information (or information that could become personal information) will be handled</p> <p>H – A significant amount of personal information (or information that could become personal information) will be handled</p>	L	
<p>Sensitivity of the information (eg health, financial, race)</p> <p>L – The information will not be sensitive</p> <p>M – The information may be considered to be sensitive</p> <p>H – The information will be highly sensitive</p>	L	
<p>Significance of the changes</p> <p>L – Only minor change to existing functions/activities</p> <p>M – Substantial change to existing functions/activities; or a new initiative</p> <p>H – Major overhaul of existing functions/activities; or a new initiative that's significantly different</p>	L	
<p>Interaction with others</p> <p>L – No interaction with other agencies</p> <p>M – Interaction with one or two other agencies</p> <p>H – Extensive cross-agency (that is, government) interaction or cross-sectional (non-government and government) interaction</p>	L	

<p>Public impact</p> <p>L – Minimal impact on the organisation and clients</p> <p>M – Some impact on clients is likely due to changes to the handling of personal information; or the changes may raise public concern</p> <p>H – High impact on clients and the wider public, and concerns over aspects of project; or negative media is likely</p>	L	
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---	--

3. Summary of privacy impact

The privacy impact for this project has been assessed as:	Tick
<p>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</p>	X
<p>Medium – Some personal information is involved, but any risks can be mitigated satisfactorily</p>	
<p>High – Sensitive personal information is involved, and several medium to high risks have been identified</p>	
<p>Reduced risk – The project will lessen existing privacy risks</p>	
<p>Inadequate information – More information and analysis is needed to fully assess the privacy impact of the project.</p>	

3.1 Reasons for the privacy impact rating

SaferCities takes privacy seriously and the SaferCities Privacy Policy applies to the Safer City Platform. With respect to livestream, SaferCities does not itself collect or retain the livestream images (personal information). However, it has responsibility to protect the integrity and access to that data. To that end, the livestream images are passed through secure and encrypted SaferCities servers hosted within New Zealand and SaferCities run a ‘zero-trust’ model on this cloud infrastructure. Access to this data by Police requires permission and meets Police Identity Management standards. Access to data for support and technical development is restricted to SaferCities technicians.

4. Recommendation

A full privacy impact assessment is not required

There is no storage of personal information and access to the livestream data containing images from CCTV installations is protected and secure.

5. Sign off

Scott Bain

Managing Director SaferCities

Signature

____/____/____
Date

Chris Wiggins

Chief Technology Officer

Name

Position (Manager)

Signature

____/____/____
Date

SaferCities Privacy Policy

SaferCities complies with the New Zealand Privacy Act 2020 (the Act) when dealing with personal information. Personal information is any information about an identifiable living person. However, a person does not have to be named in the information to be identifiable and information can become personal information when combined or linked with other information.

All SaferCities staff are required to be familiar with the 13 principles of the Privacy Act 2020 and the Privacy Breach notification process. To achieve this staff are required to undertake the following:

- Office of the Privacy Commissioner's eLearning courses: The Privacy Act 2020, Privacy Breach Reporting, and A Guide to Privacy Impact Assessments. Certificates are obtained upon successful completion of each course.
- Further Privacy Act 2020 compliance training as required.

To ensure the protection of privacy is at the heart of what we do, SaferCities uses the Privacy by Design (PbD) principles and privacy impact assessments (PIA) where appropriate when undertaking projects (see overleaf). These are considered best practice around the world.

Where a project deals with personal information, a specific privacy policy for that project will be created, setting out how we will collect, use, disclose and protect that personal information. When dealing with 3rd party data, if an actual or potential privacy breach is detected, SaferCities will notify the owning organisation of the potential breach for their remedial action and if no action is taken, consider notification of that breach to the Privacy Commissioner themselves.

Scott Bain

Managing Director, SaferCities

This Policy was last updated on 26th February 2021

Next Review due on 1st February 2022

Privacy by Design (PbD)

Seven principles:

1. Proactive not reactive; preventative not remedial. Anticipate privacy risks and mitigate.
2. Privacy as the default setting. Automatically protect personal information. Collect minimum information required and restrict access to information on a “need to know” basis.
3. Privacy embedded into design. Privacy central to core functionality and integrated into all IT systems and business processes.
4. Full functionality – positive-sum, not zero-sum. Possible to have win-win solution protecting privacy and meeting business requirements.
5. End-to-end security – full cycle protection. Apply privacy protections throughout the lifecycle of personal information in any system or process inc storage, access, use and disclosure.
6. Visibility and transparency – keep it open. Publish plain-language policy stateemnts, privacy impact assessments to assure people you have suitable protections in place. Helps build trust with stakeholders.
7. Respect for user privacy. Design solutions with customers in mind. Strong privacy defaults, appropriate notices and user-friendly options, including in operational changes.

Privacy Impact Assessment

Five key steps:

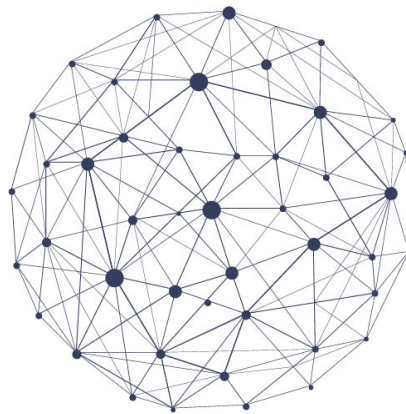
1. Define the purpose of the project and document/map out the information flows.
2. Check that your proposed collection, use and disclosure of personal information complies with the privacy principles.
3. Identify privacy risks and decide how best to avoid or mitigate them.
4. Align privacy analysis with your agency’s existing risk, information and project management methods. Determine the governance arrangements you need to support the initiative and consider any implications for third parties.
5. Produce a report that records the analysis and that can be used for decision-making.

A privacy threshold assessment is a preliminary, high level analysis that lets you see whether you need to undertake a more thorough PIA. It can help you identify and record whether your proposal raises privacy risks, assess those risks, and work out how to mitigate or manage them.



vGRID VAULT

Privacy Impact Assessment Report



August 2021

V1.2

Effective Date: 13th August 2021

Version: 1.2

Issued By: Mark McCall Consulting

Due for review: 1 August 2022

Updates	Version	Date Updated	Updated by	Approved by
Recommendations		16th August 2021	Mark McCall	Scott Bain
Action Plan		27 th January 2022	Mark McCall	Scott Bain

Privacy Impact Assessment Report – Contents

Contents	2
1. Introduction	3
2. Scope of the PIA	4
3. Personal information	5
4. Privacy assessment	7
5. Risk assessment	12
6. Recommendations to minimise impact on privacy	14
7. Action plan	15

1. Introduction

SaferCities vGRID VAULT is an application that enables Police to easily request and access CCTV footage from other organisations and the community without site visits, USBs or DVDs. Available on the NZ Police vGRID SaferCity platform, VAULT is designed to preserve police file and event numbers, while maintaining chain of evidence.

It was developed in response to the restrictions of COVID-19 lockdown preventing face-to-face visits and has been a collaboration between Police and SaferCities to design a system which meets the evidential requirements of Police.

SaferCities vGRID VAULT was launched in June 2021 and can be accessed by all Police staff who have access to vGRID SaferCity platform. Development of the project continues as feedback from users is received.

The application works as follows: Police request CCTV footage or related evidence from the public by sending a request email from VAULT. The request for assistance contains a link to VAULT and if they decide to assist Police, the person is then prompted for their details and to upload the file. As part of the Police requirements for identity of the uploader of footage, personal information by way of name, date of birth, email address, business address and telephone number is collected.

A validation of veracity is indicated by the uploader to submit the upload. An automated message of receipt is generated to the uploader containing a copy of the personal information supplied and the requesting officer and file reference number. At the same time, the officer who requested the upload is sent an alert for that submission. Only once the submission is accessed and seen by police does the personal information and digital file(s) get transmitted into the Police Enterprise network from the SaferCity data centre in New Zealand.

SaferCities vGRID VAULT has been very well received by Police as it has automated what was a face-to-face process and has saved Police and community time and resources as well as being more convenient. There are opportunities to expand its use into Police receiving other digital content via this application.

This PIA seeks to assess the privacy implications of SaferCities vGRID VAULT as it is now in operation and looking to expand to receive other digital files, and how it complies with the existing SaferCities Privacy Policy.

2. Scope of the PIA

2.1 Scope

This PIA is confined to SaferCities and the SaferCities vGRID VAULT application and its use, storage, access, retention and disposal of data within the SaferCity platform. Whilst the application is a collaboration with Police and their requirements, this PIA does not include the subsequent use of personal information accessed or downloaded by Police from the application.

2.2 The process

SaferCities staff were interviewed regarding their collaborative design process with Police Investigations team, including Police requirements for VAULT and the technical design process that included SaferCities Privacy by Design components.

SaferCities MD Scott Bain leveraged prior experience around the world over the last ten years to validate long standing issues with the community having to use USB sticks and Police having to drive to sites. Scott was also able to call on his international contacts to ratify the methodology, process flow, chain of evidence and privacy aspects of the VAULT application.

2.3 Explain the scope and process

The SaferCities vGRID VAULT application was developed in response to unique circumstances because of the COVID-19 pandemic restrictions. Although the application merely replaces a traditional, personal visit and request by Police, and is voluntary to upload footage in response to a Police request (not warrant), there is still a collection of personal information and therefore the Privacy Act 2020 applies.

Opportunities exist to enable the community to upload other digital content if requested to do so by Police, and if this function is wanted by Police, this PIA should be reviewed in light of the requested changes to confirm that for SaferCities the application complies with the Privacy Act 2020 now and with any potential future expansion. Subsequent use of personal information by Police falls under Police legislation and privacy obligations and are therefore not considered within scope of this PIA.

3. Personal information

“Personal information” is any information that is capable of identifying a living human being. It doesn’t have to be particularly sensitive or negative information.

However, the level of sensitivity and the level of impact on individuals will affect whether your information handling is likely to breach the law, or whether there are other privacy risks that need to be mitigated.

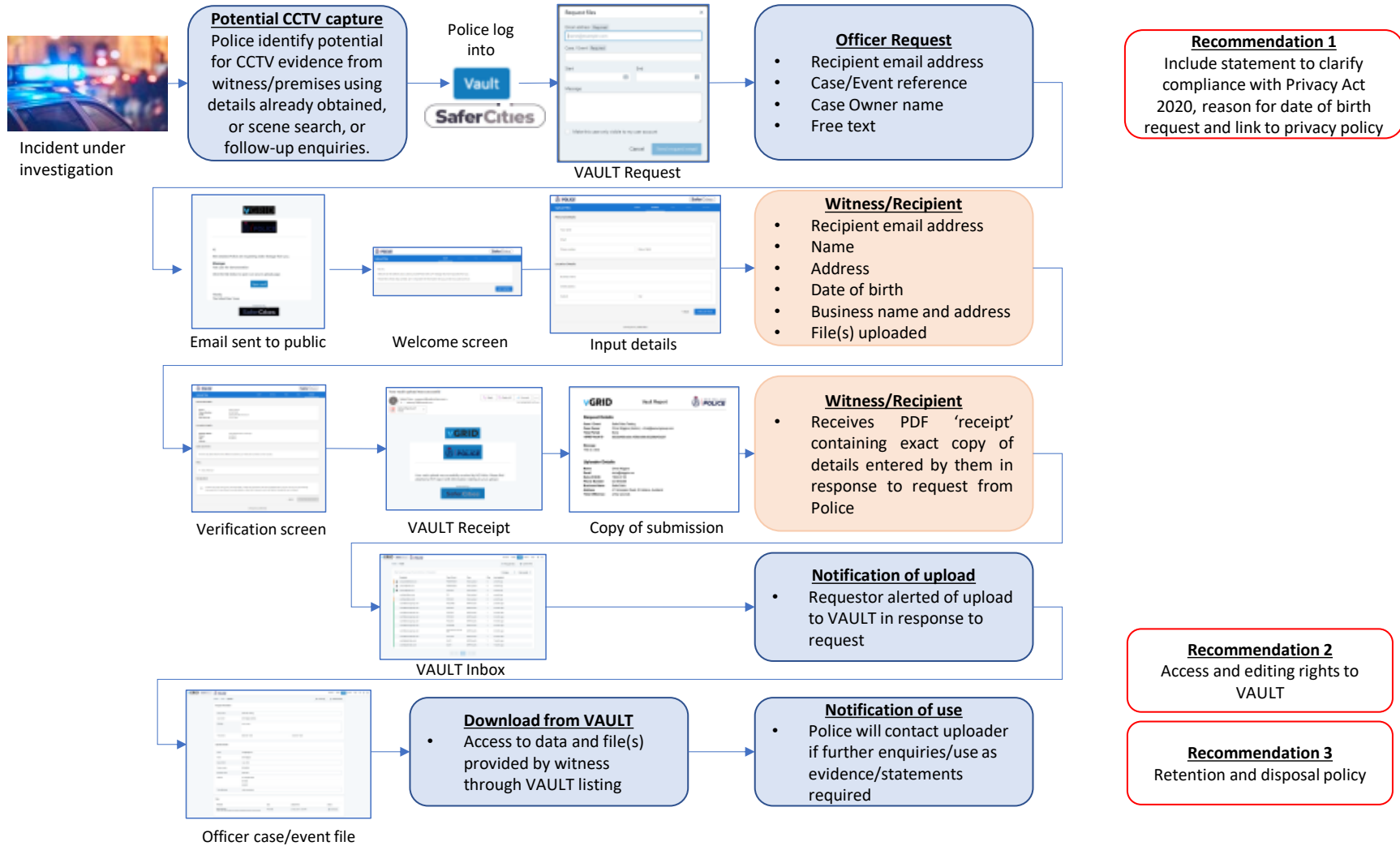
3.1 Current information flow

The SaferCities vGRID VAULT application gathers personal information in two or potentially three ways:

1. The identity of the Police member requesting any information
2. The name, date of birth, email address, business address and telephone number of the person uploading the file(s)
3. The file containing the CCTV footage itself **may** include personal information which is not know until viewed by Police.

This information flow is described in Figure 1 below.

Figure 1: SaferCities vGRID VAULT Information Flow and Privacy implications



4. Privacy assessment

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
1	<p>Principle 1 - Purpose of the collection of personal information</p> <p>Only collect personal information if you really need it</p>	<p>Personal information is collected in order to provide contact details and the identity of uploader. The information collected is: Recipient email address, name, address, date of birth, business name if relevant, and address. The requirement for date of birth is standard for Police to assist them identify the person through Police databases as well as providing the age of the uploader which may be relevant if juvenile for example.</p>	<i>Complies</i>	
2	<p>Principle 2 – Source of personal information</p> <p>Get it directly from the people concerned wherever possible</p>	<p>The information is collected directly from the uploader entering their details in a preformatted electronic form.</p>	<i>Complies</i>	
3	<p>Principle 3 – Collection of information from subject</p> <p>Tell them what information you are collecting, what you're going to do with it, whether it's voluntary, and the consequences if they don't provide it.</p>	<p>There is a free text box for the requesting Police staff member to state exactly what is being asked and why. The personal information required is stated in each input field labels. There is no explicit statement regarding it being voluntary, though not completing it is an option to opt out. There is no explanation as to what will be done re the info provided and file uploaded.</p>	<i>Complies but opportunity for improvement</i>	<i>R-1</i>

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
4	<p>Principle 4 – Manner of collection of personal information</p> <p>Be fair and not overly intrusive in how you collect the information</p>	<p>The request for information replaces what would previously been police knocking door to door or sending someone to the premises to collect any footage downloaded to a USB or DVD. The emailing of the request instead is fair and appropriate in the circumstances.</p>	<i>Complies</i>	
5	<p>Principle 5 – Storage and security of personal information</p> <p>Take care of it once you've got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.</p>	<p>SaferCities stores the data within a data centre in New Zealand. This 3rd party datacentre has security policies which comply with international standards and best practice. SaferCities staff who maintain the SaferCities vGRID VAULT application comply with the SaferCities Security Plan and policy framework.</p> <p>However, the fact that anyone in Police with access to the SaferCities vGRID platform can also log into VAULT and see and inspect the submitted entries is a concern. Police have asked for the ability to restrict viewing to the officer themselves if required, but the default remains open to view by any Police or SaferCities staff member in VAULT.</p>	<p><i>Complies but opportunity for improvement</i></p> <p>Whilst there are data protection and privacy policies for Police, and a clear audit trail of access by individual 'single sign-on', consideration of secure by default and random audit of access to entries should be discussed with Police in line with their Privacy Impact Assessment of VAULT.</p>	<i>R-2</i>

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
6	<p>Principle 6 – Access to personal information</p> <p>People can see their personal information if they want to</p>	<p>The person submitting this form is provided with a copy of their submission including the personal information they supplied, at the time of submission. Should a subsequent request be made to Police, then a copy of that receipt can be provided. Whether SaferCities vGRID VAULT is included in the Information Act request search of Police datasets needs to be explored. However, given the basic level of personal information provided this is not a significant issue.</p>	<i>Complies</i>	
7	<p>Principle 7 – Correction of personal information</p> <p>They can correct it if it's wrong, or have a statement of correction attached</p>	<p>The person enters their data directly into the fields and are then required to check box that the information is correct prior to submitting it. The copy of information submitted also requests that if anything is incorrect to contact the requesting officer so that corrections can be made.</p> <p>The Police staff member has full editing rights in VAULT to correct errors.</p>	<i>Complies</i>	
8	<p>Principle 8 – Accuracy etc. of personal information to be checked before use</p> <p>Make sure personal information is correct, relevant and up to date before you use it</p>	<p>The information is provided by the individual concerned and that person is asked to verify its accuracy upon submission by checkbox, and then is provided with a copy of the information provided and asked to contact police to make any corrections.</p>	<i>Complies</i>	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
9	<p>Principle 9 – Not to keep personal information for longer than necessary</p> <p>Get rid of it once you're done with it</p>	<p>The data provided is stored at the SaferCities datacentre and when accessed by Police through their Police Enterprise system, can be stored within the Police network. Whilst the Public Records Act 2005 legislation applies to Police holdings, SaferCities acting on behalf of Police, will hold data for periods yet to be specified. Submitted forms and CCTV file uploads which are required as evidence for Court (due to unique hash code original file identifier), will only be destroyed on direction of Police. No SaferCities policy for holding data on behalf of Police exists, other than SaferCities Privacy Policy.</p>	<p><i>Does not comply</i></p> <p>Recommend policy and process for retention and disposal of records for four use cases: Completed, Evidence; Under investigation; NFA.</p>	R-3
10	<p>Principle 10 – Limits on use of personal information</p> <p>Use it for the purpose you collected it for, unless one of the exceptions applies</p>	<p>The use of the personal information provided solely as identifying contact details for any future follow-up by Police is clear and logical.</p>	<i>Complies</i>	
11	<p>Principle 11 – Limits on disclosure of personal information</p> <p>Only disclose it if you've got a good reason, unless one of the exceptions applies</p>	<p>The personal information is disclosed to Police as intended and SaferCities is merely a technical facilitator of that disclosure.</p>	<i>Complies</i>	
12	<p>Principle 12 – Limits on disclosure of personal information overseas</p> <p>Only disclose information if adequate protection exists</p>	<p>The data is collected and stored within New Zealand and accessed by Police for their lawful purposes. Nothing is sent overseas.</p>	<i>Complies</i>	

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
13	Principle 13 – Unique identifiers Only assign unique identifiers where permitted	No unique identifier is assigned to the personal information requested in the submission. A unique hash code is applied to the file uploaded for the purposes of original exhibit.	<i>Complies</i>	

Summary / Conclusions

SaferCities vGRID VAULT has been designed in collaboration with Police to request voluntary submission of CCTV footage between specific dates/times which may help Police investigations. In doing so it requires the supply of personal information in the form of contact details, including date of birth which Police routinely collect to aid identification.

This use of personal information is uncontroversial with negligible risk of harm to an individual. The data collected is voluntary and used for subsequent contact purposes only. In many cases, the person providing the information would already have had contact with Police and be expecting to use SaferCities vGRID VAULT as an efficient and convenient process to provide Police information which may help their enquiries.

This PIA has however revealed opportunities in three areas to strengthen the privacy safeguards and ensure compliance with Principle 9, not to keep personal information longer than is necessary. These three risk areas are:

1. Provide a privacy statement on use of data and/or link to privacy policy, (Principle 3).
2. Reassess the need for access and editing of records to be available to all Police users by default, (Principle 5).
3. Have a clear retention and disposal policy for the data contained on the SaferCities servers which also meets Police evidential requirements (Principle 9).

Each of these three areas have been addressed by a risk assessment and action plan as detailed in the following sections and will require discussion and agreement with Police.

5. Risk assessment

Principle 3: Collection of personal information from the subject							
Ref. no.	Telling the individual what you're doing	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual current risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
1	Email request from Police for personal information for identification and contact purposes and upload of CCTV file	Ensuring person knows why collected, what will be done with the information, and their privacy is considered (privacy policy).	To ensure transparency and provide reassurance that their privacy matters to Police will promote trust and confidence in Police.	Reasonable request for information by Police, which would otherwise be asked in person. However, useful to explain why date of birth is requested.	Low	Include statement to clarify compliance with Privacy Act 2020, reason for date of birth request and link to privacy policy	Low
Principle 5: Storage and Security of personal information							
Ref. no.	How you are storing and securing personal information	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
2	Data stored on SaferCities server is available to view and edit to all with VAULT access by default.	Police staff with no legitimate reason to view/edit personal details can do so.	Loss of security and potentially data by mistake or design. Impact on trust.	Officers can restrict access to just themselves. Audit of access and editing is maintained by SaferCities.	Low	Restrict access to only the officer requesting as default. Allow supervisor access to override default in urgent cases. Storage of file within Police environment once downloaded.	Low

Principle 9: Agency not to keep personal information for longer than necessary

Ref. no.	How long do you keep personal information and why?	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
3	Retention and disposal policy needs to be defined. Implications for original file upload being evidence also needs to be considered.	SaferCities is relying on Police requirements for retention and authority to dispose of records and files within VAULT.	This does leave SaferCities vulnerable to breaching its own Privacy Policy and potential breaches of Privacy Act 2020.	SaferCities Privacy Policy	Medium	SaferCities should decide with Police a joint policy for retention and disposal of data stored. This should include: <ol style="list-style-type: none"> 1. Categorisation of data/file eg: NFA, ongoing investigation, evidence, completed. 2. Agreed SaferCities retention periods for each of the categories. 3. Automated reminders to Police to review status of case file. 4. Storage and retention of data and file within Police Enterprise system rather than SaferCities for these categories to be considered. 	Low

6. Recommendations to minimise impact on privacy

Ref	Recommendation	Agreed Y/N
R-1	Include statement to clarify compliance with Privacy Act 2020, reason for date of birth request and link to privacy policy	Y
R-2	Restrict access to only the officer requesting as. Allow supervisor access to override default in urgent cases. Storage of file within Police environment once downloaded.	Y in principle
R-3	<p>SaferCities should decide with Police a joint policy for retention and disposal of data stored. This should include:</p> <ol style="list-style-type: none"> 1. Categorisation of data/file eg: NFA, ongoing investigation, evidence, completed. 2. Agreed SaferCities retention periods for each of the categories. 3. Automated reminders to Police to review status of case file. 4. Storage and retention of data and file within Police Enterprise system rather than SaferCities for these categories to be considered 	N

7. Action plan

Ref	Agreed action	Who is responsible	Completion Date
A-1	Update screens to include privacy purpose information	CW	15 th February 2022
A-2	Discuss with Police to make restriction to officer requesting as default. Police requested it to be open as default to enable colleagues in investigating team to access during absence/off duty of originating officer.	SB	10 th February 2022
A-3	In the absence of Police direction, SaferCities Privacy Policy will apply, and data will only be stored for 30 days.	SB	31 st March 2022