

29 June 2026

Miss M Quicken
fyi-request-33843-cabf393c@requests.fyi.org.nz

Tēnā koe Miss Quicken

Request for information

Thank you for your Official Information Act 1982 (OIA) request of 24 February 2026, in which you asked for information regarding the On Duty App.

On 27 April 2026 you provided clarification of your request, my response to each part of your request can be found below.

1. a) *The current assessments including impact assessments relating to OnDuty app.*

Clarified to:

What specific assessments or impact assessments you are seeking in relation to the OnDuty app (for example, whether these relate to human rights, privacy, operational, security, or other matters)

Priority is with human rights & privacy. There are multiple aspects and these should have been released proactively when the police adopted the posture with onDuty app.

Impact Assessments other than human rights & privacy typically have scope & sections relating to human rights & privacy on their impact so generally these should be included as part of the request.

Specific human rights assessments were not completed for the OnDuty software application either at the time of implementation, or in the intervening period. Accordingly, this aspect of your request is refused under section 18(e) of the OIA, as the information requested does not exist.

A Privacy Impact Assessment (PIA) for the OnDuty application was completed in April 2018. Given the changes in the law and technology since then, the PIA should only be considered as a 'historical assessment only'. The lens that was used in the 2018 assessment may be different to the approach that might be taken if a similar assessment was undertaken today.

A copy of the Privacy Impact Assessment is enclosed in response to this request.

No further Privacy Impact Assessments have been completed since 2018.

2. b) Access control assessment that has been done to protect it from unauthorized use.

Clarified to:

What [do] you mean by an “access control assessment” (for example, whether you are seeking a formal assessment document, a summary of controls, or another type of information)

This is a standard document trail that gets done as part of the reviews when any new technology is introduced that has an impact to safety & privacy of general public.

Access control is meant to mitigate and / or limit the mis-use of the system outside it's intended scope.

There is significant history internationally where staff members of police have mis-used information collected and even sold the information to bad actors.

Yes, the ones you have listed are typically included as are documents that ensure the implementation ensures mis-use is minimized if not eliminated.

Access to OnDuty is restricted to users specified on the Police Active Directory. This access list includes primarily Constabulary police members, and selected Police Employees who have a business reason to access the applications controlled by the Police Active Directory.

Access Control is considered as part of the Security Risk Assessment process. A Security Risk Assessment for OnDuty was completed in September 2021, which has been released in response to this request.

Portions of the Security Risk Assessment, including Appendix 1, are withheld under section 6(c) of the OIA, as the release of the material would likely prejudice the maintenance of the law, including the prevention, investigation, and detection of offences.

3. c) The list / spreadsheet of all the parties that are linked to the system e.g. data exchange and their relevant statutory enabled privacy commissioner vetting.

Clarified to:

What level of detail you are seeking in relation to third parties linked to the system, and what do you mean by “statutory enabled Privacy Commissioner vetting”.

<https://www.privacy.org.nz/about-us/information-sharing/information-matching/>

When and if you receive or send data from / to another agency there is a specific statutory requirement to do this vetting.

<https://www.legislation.govt.nz/act/public/2020/0031/latest/whole.html#LMS23752>

I am asking the evidence that you both listed where the information is sent and from which other sources you used which are liable to this statutory requirement.

And that you followed the process with the privacy commissioner as is required given the sensitivity of the data.

Also just to clarify one more point.

*What level of detail you are seeking in relation to third parties linked to the system

I would like to have

- The organisation name*
- Start & end dates and;*
- What classification / type of information is either matched, received or shared*
- Is information matching used and what identifiers are used to match?*
- Is the data being sent to the organization ?*
- Is the data being received by the organization ?*

A table setting out OnDuty links with organisations is enclosed. In that table you will note a reference to the Family Safety System (FSS).

FSS is not an external organisation. FSS is a Police hosted multi-agency software application to which many organisations have access. Some of these include:

- Department of Corrections
- Ministry of Education
- Health New Zealand - TeWhatu Ora
- ACC
- Oranga Tamariki
- Women's Refuge
- Iwi providers

It should be noted a security model allows access only to information that is relevant to that agency or Non-Governmental Organisation (NGO) to conduct their role for any given family harm incident.

Further information regarding how we manage personal information is available on the Police website here:

[Privacy statement - how we manage personal information | New Zealand Police](#)

Information specific to the Family Safety System can be found under the *Disclosing and sharing personal information* section.

The Privacy Act 2020 does not include a statutory vetting regime in respect to authorising parties to access Police systems or to share information with Police.

Police must ensure that any access granted, or sharing of information is consistent with the Privacy Act 2020 or is otherwise authorised under NZ law.

Memorandum of Understandings (MOUs) between Police and other New Zealand agencies formalise information sharing however the Privacy Act 2020 does not include a statutory requirement to consult MOUs with the Privacy Commissioner.

Police is cognisant of the requirement to comply with the Cabinet Manual and recognises it may sometimes be needed to consult with the Privacy Commissioner as part of the policy development process (Cabinet Manual, clause 5.19).

Please note that as part of its commitment to openness and transparency, Police proactively releases some information and documents that may be of interest to the public. An anonymised version of this response may be publicly released on the New Zealand Police website.

You have the right to seek an investigation and review by the Ombudsman of the decision to withhold any information. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Nāku noa, nā

A handwritten signature in blue ink, appearing to be 'LC' followed by a stylized flourish.

Inspector Luke Cameron
Product Manager, Mobility and Deployment
New Zealand Police

Organisation Name	Start Date	End Date	Classification/Type of information	Received/Shared	Is Information Matching Used?	What Identifiers Are Use To Match Data?	Comment
New Zealand Land Transport Agency	Exact date not known	Current	Commercial Vehicle Investigation Traffic Crash Reports Driver photos	Shared (Sent) by Police	No data matching undertaken in OnDuty	N/A	
Family Safety System (FSS)	Exact date not known	Current	Details from the Family Harm report including: List of person involved and their name, phone number, ethnicity, gender Public Safety Order issued: Yes/No Source (Always Police) Police Station Event no Dynamic Risk Assessment (DYRA) Score DYRA content Reported date Incident code Reported by Scene address Proximity: (At/Near) Scene Type Firearm: Yes/No Alcohol:Yes/No Drugs: Yes/No Summary (Family Harm narrative)	Shared (Sent) by Police	No data matching undertaken in OnDuty	N/A	Family Safety System (FSS) is not an an external agency. FSS is a Police hosted multi-agency application to which organisations including Department of Corrections, Ministry of Education, Health New Zealand - TeWhatu Ora, ACC, Oranga Tamariki, Womens Refuge and Iwi providers have access to. It should be noted that a security model allows access only to information that is relevant to that agency or NGO to conduct their role for any given family harm incident.
New Zealand Post	Exact date not known	Current	A PDF of the Infringement Offence Notice including: Date Day Time Driver details Vehicle details Offence details Location details Payment details	Shared (Sent) by Police	No data matching undertaken in OnDuty	N/A	
Auror	Exact date not known	Current	Date and time details Organisation details Reporter details Event details Person details Vehicle details Photos Location details	Received by Police	Data matching undertaken in OnDuty	Name Date of Birth Gender Address	Note that not all of these attributes are visible in the user interface ('front end') of the application.
Auror	Exact date not known	Current	DOCLOC (Police file number)	Shared (Sent) by Police	No data matching undertaken in OnDuty	N/A	
Immigration New Zealand	Exact date not known	Current	Photos Person details		No data matching undertaken in OnDuty	N/A	OnDuty includes the ability to launch a query of Immigration New Zealand (INZ) and Department of Internal Affairs (DIA) databases. Information from INZ of DIA is not ingested by OnDuty but simply presented for the user.
Department of Internal Affairs	Exact date not known	Current	Passport information Births Deaths and Marriages information				OnDuty includes the ability to launch a query of Immigration New Zealand (INZ) and Department of Internal Affairs (DIA) databases. Information from INZ of DIA is not ingested by OnDuty but simply presented for the user.
Oranga Tamariki	Exact date not known	Current	Child Protection Protocol report Family Harm Report	Shared (Sent) by Police	No data matching undertaken in OnDuty		

System	Mobility Platform including OnDuty application
Date	September 2021
Facilitator	Michelle Soper (Mobility/Digital Project Manager) and Jay Garden (CISO)

Purpose

The purpose of this Security Risk Assessment (SRA) report is to document the information security risks, controls and treatments associated with the Mobility platform, including the OnDuty application.

System and Project Background

The Mobility platform continues to be a key enabler to NZ Police to deliver frontline services and has been since iPhones were first rolled out to NZ Police frontline staff in 2013. NZ Police ICT (Public Safety Network, ICT Operations & Mobility/Digital group) is responsible for the operational management of the Mobility platform with support from vendor Vodafone.

The NZ Police Mobility Programme developed a bespoke iPhone application for frontline officers called OnDuty, with the first version implemented in 2015, and ongoing enhancements and additional features added over 2016-2021. OnDuty is an operational application that provides query, tasking and reporting capability.

OnDuty has transformed the way frontline police collect, access and act on information. The objective of OnDuty is for NZ Police staff to have the right information at their fingertips straight away, so they're able to make better decisions in real-time situations.

There were previously a series of overlapping assessments completed in the early days of the Mobility programme (over 2011 to 2013). These were used as the starting point for this SRA, in preparation for seeking renewal of Certification and Accreditation of the Mobility platform, including the OnDuty app.

The scope of this SRA is:

1. The Mobility platform consisting of:
 - Physical iPhones (there are 11,860 Police iPhone XRs currently in use across NZ Police);
 - Operational management of the iPhone fleet and the applications on them; and
 - Mobility infrastructure (hardware, software, operating systems) that support the management of the iPhones and the applications on them.

Note: The responsibility for some aspects of Mobility operational management have moved within ICT from the Mobility/Digital Group to the Public Safety Network group as of 1 Sept 2021.

2. The OnDuty application: OnDuty was developed by the NZP Mobility programme in conjunction with the National Intelligence Centre, Police ICT and external vendor Smudge, and implemented on iPhones in December 2015. The initial release was just for Road Policing staff to query persons, vehicles and organisations. Over 2016-2021 the Mobility Programme (now Mobility/Digital Group) have continued to evolve and expand the OnDuty app.

OnDuty consists of an iPhone-based 'OnDuty' App, a back-end OnDuty database, and a desktop 'OnDuty Office' and 'OnDuty FMC' app. Some data is retained in the OnDuty database, but most data collected via OnDuty is submitted and stored in other systems and 'mastered' in those other systems (NIA, PIPS, NZTA CAS, PROP, BMA and others).

OnDuty currently (Aug 2021) includes the following features:

- QP, QV, QO, QL, QI (Queries)
- FH (Family Harm)
- INF (Infringement Notice Form)
- TCR (Traffic Crash Report)
- CVIR (Commercial Vehicle Inspection Report)
- N (Notings)
- OR (Offence Report)
- WS (Warrantless Search)
- HR (Health Referral - Drug Use)
- PF (Property Form)
- GCR (Gun Club/Range Visit)
- PoE (Place of Education Visit)
- PoW (Place of Worship Visit)
- S118 (s118 Letter)
- Bail
- There is also external agency information available in OnDuty
 - NZTA photos in OnDuty
 - Immigration New Zealand (INZ) data
 - Department of Internal Affairs

There are approximately 10,000 users of OnDuty (of which 8000 are regular users).

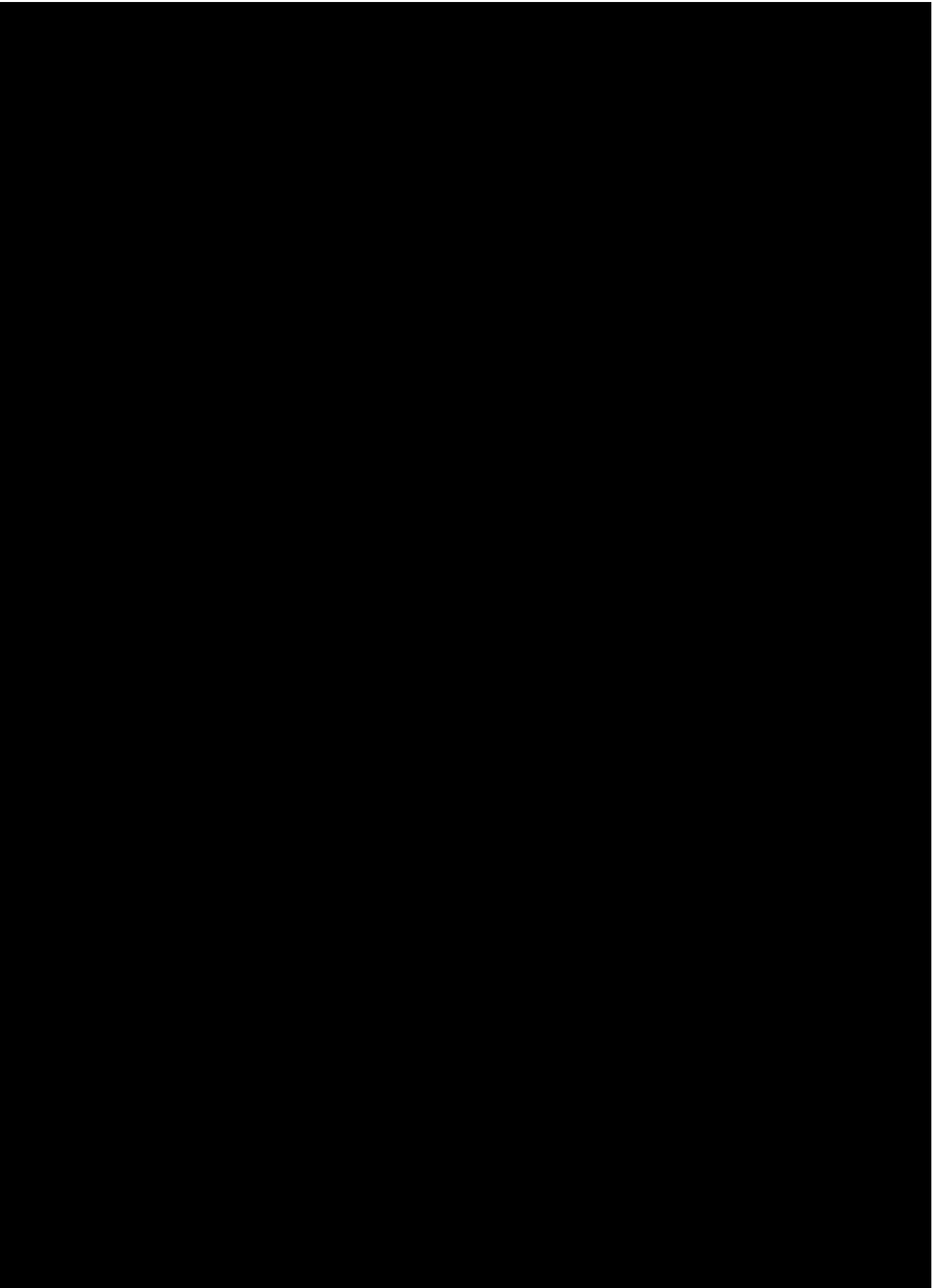
The information in the Mobility platform and OnDuty app includes SENSITIVE / RESTRICTED.

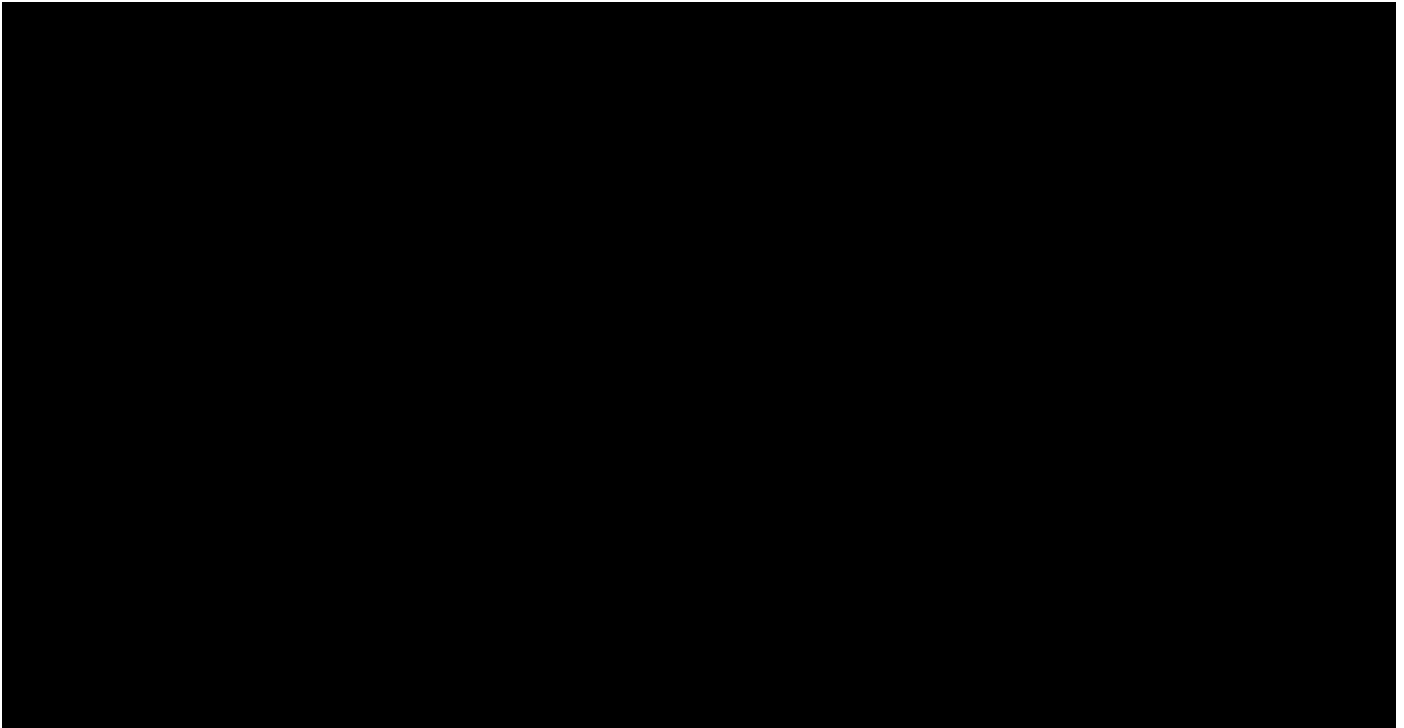
See Appendix 3 for an overview diagram of the Mobility infrastructure including OnDuty.

Risk Summary

This risk assessment was carried out in accordance with the Police Risk Management Framework. A risk workshop was held on 21 & 26 January 2021 with the following stakeholders and subject matter experts:

- Mark Donaldson, Deputy Director Mobility/Digital
- Kate Witchell, A-Product Manager Mobility/Digital
- Michelle Soper, Project Manager, Mobility/Digital
- Sam Holmes, Application Developer, Mobility/Digital
- Greg Lintott, Solutions Architecture
- Kerry Burke, Application Developer, Absolute IT
- Cliff Clark, Cybersecurity Manager
- Jay Garden, Chief Information Security Officer
- Ian Gallagher, ICT Operations Manager, Applications Support
- Janet Thomson, ICT Service Delivery Manager – Mobility
- Sandra Bateman, Developer, Smudge
- Chris Brown, Lead Developer, Smudge





<i>Endorsement</i>	<i>Representing</i>	<i>Endorsement date</i>
Brian Moyle	Sponsor – Dir. Mobility/Digital	23 September 2021
Mark Donaldson	Deputy Dir Mobility/Digital	29 September 2021
John Nixon	Programme Manager Mobility/Digital	21 September 2021
Dylan Earle	Public Safety Network	16 September 2021
Greg Lintott	ICT Architecture	20 September 2021
Janet Thomson	Mobility Service Delivery Manager	29 September 2021
Ian Gallagher	ICT Operations, Application Support	29 September 2021
Annabel Fordham	Privacy	24 September 2021
Cliff Clark	Cybersecurity	30 September 2021
Jay Garden	Info Assurance	16 September 2021

<i>Approval by Business Owner</i>	<i>Approval date</i>
Steve Pyne, Acting Chief Information Officer	2 November 2021

Appendix 1: Risk Review

See the attached Spreadsheet for the details of the risks identified and assessed in the risk workshop. It includes the risk levels and ratings for inherent (untreated) and residual risks, and details the associated treatments identified for each risk.

Appendix 2: Police Risk Management Tables

CONSEQUENCE TABLE

Determine the consequence of the unexpected event

	NEGLECTIBLE	MINOR	MODERATE	MAJOR	SEVERE
Our people	Concerned or unhappy staff.	Difference of opinion and poor performance leading to waste or rework.	Low morale and de-motivated staff.	High levels of dissatisfaction across district or part of organisation.	Personal grievances and multiple staff resignations.
Goals & objectives	Would have little if any effect on goals and objectives.	Would threaten a component or part of the goals and objectives.	Would threaten goals and objectives.	Would necessitate serious adjustment to the overall goals, objectives and/or plans.	Would have permanent impact on achievement of goals and objectives.
Our reputation	Local mention only. Quickly forgotten. Freedom to operate unaffected. Self-improvement review required.	Scrutiny by Executive, internal committees or internal audit to prevent escalation. Short term local media concern. Some impact on local level activities.	Persistent national concern. Scrutiny required by external agencies. Long term 'brand' impact.	Persistent intense national public, political and media scrutiny. Long term 'brand' impact. Major operations severely restricted.	International concern. Governmental inquiry or sustained adverse national/international media. 'Brand' significantly affects organisational abilities.
Service delivery	Infrequent and inconsequential disruption to core services.	Temporary disruption to core services at a local level.	Inability to provide or maintain core services at a local level.	Inability to provide or maintain key infrastructure of a widespread nature.	Inability to provide or maintain key services for significant periods of time.
Wellness and safety	First aid treatment required. No down time. Near misses.	Medical treatment required in single figures. Down time.	Significant down time and possible long term disabilities.	Death of individuals, extensive injury and hospitalisation.	Death of multiple staff, public or others outside Police.
Information, privacy and security	Compromise or corruption of information held that is otherwise available in the public domain.	Compromise of information that could impact upon internal or sub-unit interests.	Compromise of information that could impact upon the organisation's daily operations.	Compromise of information sensitive to organisational interests.	Compromise of information with significant ongoing impact.
External relationships	Disruption to service delivery and debate on approach.	Disruption to service delivery and disagreement on approach.	Disruption to service delivery and strained relationships.	Serious disruption to service delivery and fracturing of relationships.	Halt to service delivery and termination of relationship.
Financial impact	Slight financial issue managed by repositioning within financial baseline.	Adverse financial impact requiring financial repositioning.	Significant financial impact requiring central (internal) resource funding.	Serious financial implications requiring significant financial repositioning.	Grave financial implications necessitating new Crown funding or major service cutbacks.
Project/programme delivery	A delay, cost increase or scope change for a specific deliverable that doesn't impact on overall delivery.	A delay, cost increase or scope change for a number of deliverables that doesn't impact on overall delivery.	A delay to the timetable or change to the scope that results in less than 3 months of delays.	A three month or longer delay due to the timetable, scope or benefits changing.	A scope, cost or timetable change that fundamentally changes the project making it no longer viable.

The headings and descriptors are not prescriptive or exhaustive and are meant as a guide only.

RISK LIKELIHOOD TABLE

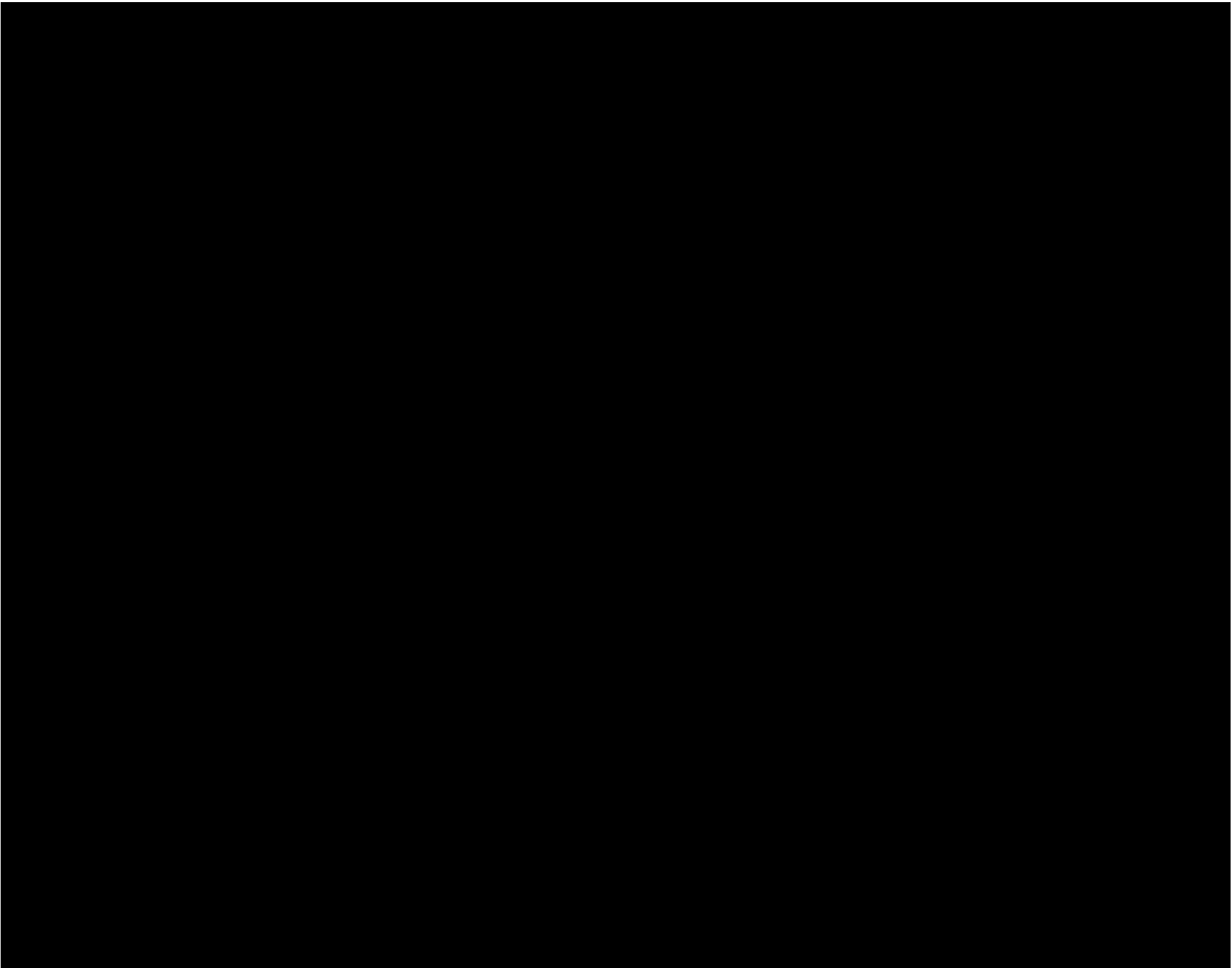
Determine the likelihood of the unexpected event

LIKELIHOOD	PROBABILITY	CHANCE
Almost certain	>95%	The event will occur in most circumstances
Likely	>65%	The event will probably occur in most circumstances
Possible	>35%	The event might occur at some time
Unlikely	<35%	The event could occur in some circumstances
Rare	<5%	The event may occur in some exceptional circumstances

RISK MATRIX

Your consequence and likelihood leads you to your risk rating

		CONSEQUENCE				
		NEGLECTIBLE	MINOR	MODERATE	MAJOR	SEVERE
LIKELIHOOD	ALMOST CERTAIN	11	16	20	23	25
	LIKELY	7	12	17	22	24
	POSSIBLE	4	6	14	18	21
	UNLIKELY	2	5	9	13	19
	RARE	1	3	6	10	15
Risk key:		Low risk	Medium risk	High risk	Very high risk	





OnDuty
Privacy Impact Assessment
7th April 2018



INFO by Design

It's about them - putting your customers at the centre
of how you manage their information



Contents

A. INTRODUCTION AND PURPOSE	3
B. PROJECT SUMMARY	3
OVERVIEW	3
EXPECTED BENEFITS	3
C. SUMMARY ANALYSIS.....	4
D. INDIVIDUAL AND STAKEHOLDER IMPACTS	4
E. INFORMATION OVERVIEW	4
QUERIES	4
INFRINGEMENT OFFENCE NOTICES (IONS) AND WRITTEN TRAFFIC WARNINGS (WTWs)	5
TRAFFIC CRASH REPORTS (TCR)	6
COMMERCIAL VEHICLE INSPECTION REPORTS (CVIR)	7
NOTINGS	7
FAMILY HARM INVESTIGATIONS.....	8
F. ASSESSMENT OF PRIVACY IMPACTS	9
COLLECTING OR OBTAINING INFORMATION.....	9
STORAGE, SECURITY AND RETENTION	10
ACCESS AND CORRECTION	10
ACCURACY	10
USE AND DISCLOSURE.....	11
UNIQUE IDENTIFIERS	12
G. MANAGEMENT APPROACH	12
INFORMATION SHARING.....	12
USE OF INFORMATION IN NON-PRODUCTION ENVIRONMENTS	12
ACCURACY	13
H. REQUIRED PRIVACY CONTROLS	13

A. Introduction and Purpose

1. Family Harm Investigations are shortly going to be included into the OnDuty solution as part of the Mobility Programme. A Privacy Impact Assessment (PIA) is being completed at this time to ensure that any privacy issues are identified prior to release.
2. There is not currently a PIA covering the existing components of the OnDuty solution. The scope of this assessment has been expanded to cover the OnDuty solution as a whole, with specific consideration of the changes being implemented to include Family Harm Investigations.
3. This PIA will consider the entire information lifecycle, including:
 - Collecting or obtaining information
 - Storage, security and retention
 - Access and correction
 - Accuracy
 - Use and disclosure
 - Unique identifiers.
4. This PIA has been developed based on:
 - Documentation provided by NZ Police
 - Walkthroughs of the solution
 - Meetings with key NZ Police personnel.

B. Project Summary

Overview

5. Mobility is a fundamental enabler for New Zealand Police to deliver their services. The Mobility Action Plan to 2021 sets out their smartphone technology aspirations for the next five years that will enable frontline staff to be more mobile, visible, informed and effective than ever before.
6. The Mobility Programme in conjunction with the National Intelligence Centre, Police ICT and Smudge Apps developed the application OnDuty.
7. In December 2015, OnDuty was introduced to Road Policing staff providing them the ability to query persons, vehicles and organisations.
8. In mid-2016, OnDuty was rolled out to all Police staff providing them the ability to issue Infringement Offence Notices (IONs), Written Traffic Warnings (WTWs), Traffic Crash Reports (TCRs) and Commercial Vehicle Inspection Reports (CVIRs) using the OnDuty app on their mobility device.
9. Development in OnDuty has continued with Notings being rolled out to all users in May 2017, as well as the introduction of query item and the set up of the OnDuty Service Improvement Team (OSIT).
10. Currently an enhancement to OnDuty is being developed to enable the inclusion of Family Harm Investigations. This functionality is expected to go live in June 2018.

Benefits

11. The current and anticipated future benefits of OnDuty are :
 - Frontline Officers will be enabled to provide more effective and efficient services by being more visible within their communities and less time in their offices. The electronic workflow reduces double handling and improves data capture and consequently data quality.

- Frontline Officers feel more confident having the tools, resources, systems and processes to do their job well.
- NZ Police Staff, partners and sector agencies feel more confident making decisions based on good quality information.
- The mobility solution contributes to improving NIA data quality.

C. Summary Analysis

12. In general, the remaining privacy risks related to the use of OnDuty are considered low and able to be mitigated by transparent communications and robust security arrangements.
13. Risks exist around information sharing, use of production information in non-production environments and accuracy of the information. Recommended controls to address possible risks are set out at the end of this PIA. The controls include updating privacy notices and providing written copies longer term to families involved in a Family Harm Investigation. It is also recommended that a Certification and Accreditation is completed on the non-production version of OnDuty to ensure all controls are functioning effectively.

D. Individual and Stakeholder Impacts

14. OnDuty is used to collect information about people, places, and incidents. This information is then utilised to:
 - To inform a range of police staff, including the ability for frontline staff to consume that information in near real time. Record events within other Police systems such as NIA and the Police Infringement Processing System (PIPS).

Information recorded within OnDuty may be shared with the following third parties as part of normal Police business:

-
- NZTA
- NZ Post
- Integrated Safety Response (ISR) agencies.

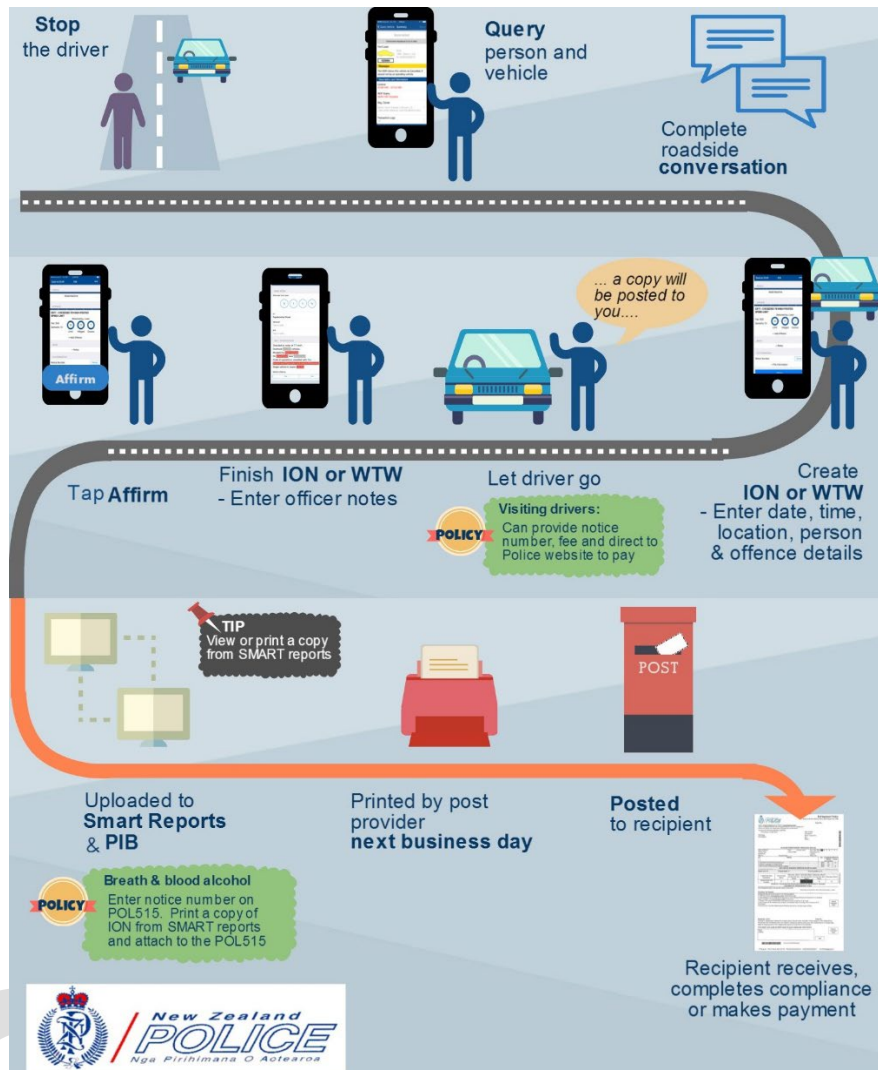
E. Information Overview

Queries

15. When completing queries, Officers can search:
 - Vehicles (QV)
 - Person (QP)
 - Location (QL)
 - Item (QI)
 - Organisation (QO)
16. The queries return details currently held by Police in NIA.
17. The detailed queries are maintained on the Officer's mobility device and in their history for thirty days post submission to allow them to refer to them if required. Queries can also be saved into a folder to allow the Officer to then link them to other records such as IONs. This reduces the need for re-entry of information by Officers.

Infringement Offence Notices (IONs) and Written Traffic Warnings (WTWs)

18. The following shows the information flow relating to IONs and WTWs.



19. When issuing IONs and WTWs the following information is collected:

- Date
- Time
- Location
- Driver details
- Vehicle details
- Offence details
- Officer notes.

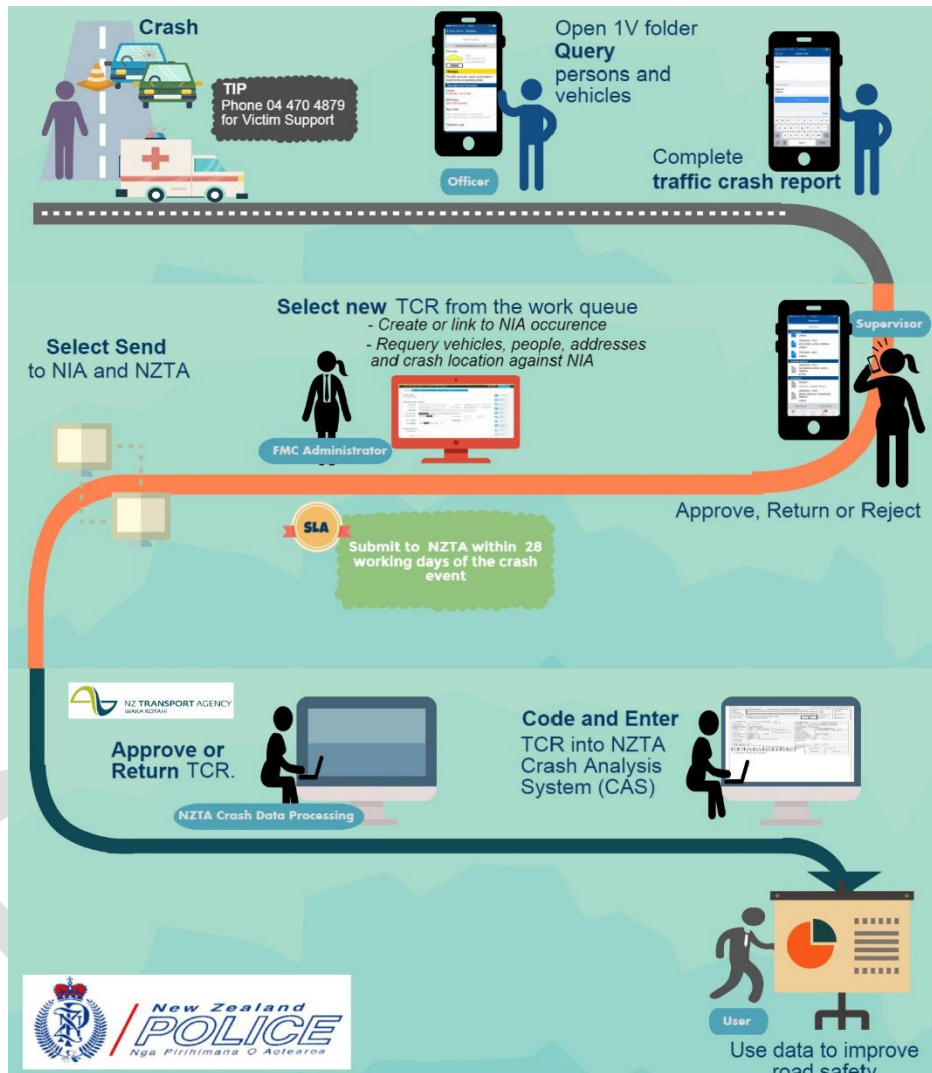
20. The driver and vehicle details are first queried to allow the Officer to confirm they have the appropriate people and vehicles, and are aware of any information of interest. Once the Officer completes the ION or WTW the information is submitted and is passed to the Police Infringement Processing System (PIPS). Any information that doesn't adhere to the PIPS data structure the ION is entered manually by a Administration Officer at the Police Infringement Bureau (PIB)..

21. Overnight a batch file of the IONs and WTWs is passed to NZ Post who print and send the relevant notices and warnings.

22. The details of the ION or WTW are maintained on the Officers mobility device for thirty days post submission to allow them to refer to it if required. This reduces the need for re-entry of information by Officers.

Traffic Crash Reports (TCR)

23. The following shows the information flow relating to TCRs.



24. When completing a TCR the following information is collected:

- Date
- Time
- Location
- Driver details
- Passenger details
- Vehicle details
- Crash details
- Witness details
- Officer notes

- Event details
 - Environment and road conditions
 - Narrative
 - Pedestrian details
 - Crash diagram
 - Witness details
 - Outcome
 - File information.
25. The driver and vehicle details are first queried to allow the Officer to confirm they have the appropriate people and vehicles and are aware of any information of interest, unless the driver is not known at this time. Once the Officer completes the TCR the information is submitted and is passed to the Officer's supervisor for review when the Officer is next in mobile reception. If approved the TCR is then transferred to FMC who validate the information contained and link it to any existing records within NIA.
 26. Once the information is entered into NIA it is then passed to NZTA who then key the crash details into the NZTA Crash Analysis System (CAS). This process remains unchanged from the process prior to the launch of OnDuty.
 27. Once completed, the details of the TCR are maintained on the Officers mobility device for thirty days post submission to allow them to refer to it if required and provide any updates. This reduces the need for re-entry of information by Officers.

Commercial Vehicle Inspection Reports (CVIR)

28. When completing a CVIR the following information is collected:
 - Date
 - Time
 - Location
 - Driver details
 - Operator details
 - Vehicle details
 - Load details
 - Vehicle defects
 - Logbook Reference
 - Notes
 - File Information.
29. The driver, vehicle and operator details are first queried to allow the Officer to confirm they have the appropriate people and vehicles, and are aware of any information of interest. Once the Officer completes the CVIR the information is submitted and is passed directly into SMART Reports when the Officer is in mobile reception.
30. Overnight the information is passed as part of a batch to NZTA. This process remains unchanged from the process prior to the launch of OnDuty.
31. The details of the CVIR are maintained on the Officers mobility device for thirty days post submission to allow them to refer to it if required and provide any updates. This reduces the need for re-entry of information by Officers.

Notings

32. When completing a Noting the following information is collected:

- Date
 - Time
 - Location
 - Noting type
 - Reporting channel
 - Reliability of information
 - Updated person details
 - New person details including body markings details
 - Child Offenders Protection Register (COPR) details
 - Narrative.
33. The Officer is able to add persons, vehicles and organisations to Notings. It is also possible to link objects.
34. The person and / or location are queried, if applicable, to allow the Officer to retrieve the current information held by Police in NIA. Once the Officer completes the Noting it is then sent directly to NIA when the Officer is next in mobile reception, unless a new person, address or vehicle has been added. If a new object is added, the Noting is transferred to FMC who validate the information contained and link it to any existing records within NIA.
35. Once the information is entered into NIA, the Noting is used to update existing held records. The information is not shared with any third party at this time.
36. The details of the Noting are maintained on the Officers mobility device for thirty days post submission to allow them to refer to it if required and provide any updates. This reduces the need for re-entry of information by Officers.

Family Harm Investigations

37. When creating a Family Harm Investigation, the following information is collected:
- Occurrence details
 - People who are involved
 - Dynamic assessment and safety plan
 - Roles and offences
 - Location
 - Vehicles
 - Offences / Incidents
 - Narrative.
38. The people's details are first queried to allow the Officer to confirm they have the appropriate items. Once the Officer completes the Family Harm Investigation the information is submitted and is passed to the Officer's supervisor for review when the Officer is next in mobile reception. If approved the Investigation is automatically uploaded to NIA. Any information that doesn't adhere to the NIA data structure is passed to the File Management Centre (FMC) who resolve the issues as per current process.
39. Once approved the Family Harm Investigation is also provided to the Integrated Safety Response (ISR) Content Management Systems (CMS). ISR is a multi-agency initiative to ensure the immediate safety of victims and children, and to work with perpetrators to prevent further violence. Details held within the ISR CMS are used by multiple agencies to prepare Family Harm Investigations for the daily Safety Assessment Meetings (SAM).
40. The details of the Family Harm Investigation are maintained on the Officers mobility device for thirty days post submission to allow them to refer to it if required and provide any updates.

F. Assessment of Privacy Impacts

41. This section provides the detailed analysis of the privacy impacts regarding OnDuty. Identified risks will be examined in section G below.

Collecting or Obtaining Information

42. Information that is input into OnDuty is sourced from the individuals concerned (or their legal guardians if under 18).
43. Most information required to be input into OnDuty is authorised by law and must be provided when requested. The exceptions to this are witnesses details and family details relating to those who have not been arrested. These are provided with the person's consent.
44. The Land Transport Act 1998 gives Officer's powers to:
- Demand drivers provide details of their full name, address, date of birth, occupation and phone number, as well as any other details needed to identify the person.
 - Require passengers to provide information to assist in the identification of the driver.
 - Inspect the driver's licence, vehicle warrant of fitness and other official land transport document.
 - Demand drivers provide the name and address of the owner of the vehicle and the vehicle's registration number.
 - Inspect a vehicle for roadworthiness.
45. Police also have powers under the Policing Act 2008 to require passengers to provide their information if they think they have aided the driver to commit a crime.
46. Principle 3 of the Privacy Act says that, where an agency collects personal information directly from an individual, the agency must take reasonable steps to ensure that the individual is made aware of the intended recipients of the information.
47. Police's privacy notice is available on their website <http://www.police.govt.nz/about-us/how-we-manage-personal-information>.
48. Officers are also required to tell individuals how their information will be used when provided for inclusion in OnDuty. Police training materials detail these requirements. At this time Officers advise individuals that their information will be shared with other parties as part of the process.
49. The information sharing involved with Family Harm Investigations is wider stretching than for other features within OnDuty and involves multiple government agencies and non-government organisations. Currently during Family Harm Investigations, families are left with written information that included a copy of a privacy notice detailing who their information would be shared with and for what purpose. When Family Harm Investigations are recorded in OnDuty the family will no longer receive this written information, including the privacy notice. The design at time of review did not include a clear replacement for this written notice and therefore nothing advising the family of who their information would be shared with and for what purpose.

R01. There is a privacy risk that individuals are not well enough informed that their information will be shared with other agencies as a result of Family Harm Investigations.

Storage, Security and Retention

51. When accessing OnDuty the Officer must input their username and password prior to being granted access. Information held at rest is secured utilising technology solutions provided as standard with all Police mobility devices. There are also several policies relating to how Officers must secure and manage their device. Police mobility devices have a current Certification and Accreditation (C&A) confirming they meet the requirements of the New Zealand Information Security Manual (NZISM).
52. All information is transferred securely from the Officer's mobility device to internal police systems, using virtual private networks (VPNs). OnDuty has been reviewed and has a current C&A. The inclusion of the new Family Harm functionality will have been reviewed by the Technical Consultants Forum prior to go live and the C&A extended if required.
53. The Integrated Safety Response (ISR) system that Family Harm Investigations are shared with has been reviewed and a qualified C&A issued. The C&A is qualified due to some missing documentation and this does not affect its operational security.
54. NIA receives a copy of information input into OnDuty¹. NIA has a current C&A. Information is retained within NIA in accordance with the retention schedule for NIA.
55. Production information is used within the non-production environment of OnDuty. This environment is not subject to the same C&A process as production therefore it is unknown if the controls to safeguard the personal information in this environment are functioning effectively.

R02. There is a privacy risk that information relating to individuals is not appropriately secured within non-production environments.

57. Information regarding all paperwork types is stored on the Officer's mobility device for a period of thirty days post submission. This allows the Officer to recheck any details or provide updates as required when further information becomes available. After thirty days the information is no longer available via OnDuty.

Access and Correction

58. Individuals are able to access their information in accordance with the Privacy Act. Individuals are required to prove their identity when making a privacy request and complete the following form <http://www.police.govt.nz/about-us/publication/request-personal-information-form>. The introduction of OnDuty has not altered this process.
59. If an individual wishes to correct their personal information collected or held in OnDuty the person can utilise the existing correction processes. The introduction of OnDuty has not altered this process.

Accuracy

60. Information is collected directly from the individual which provides the Officer the opportunity to clarify items such as spelling of names.

1. _____

1. ¹ With the exception of some ION, WTW and CVIR information.

61. Officers also have the ability within OnDuty to scan the barcode on the individual's drivers licence to enable the person's record to be accurately located. Therefore, reducing the risk of human error on input.
62. For vehicle details the Officer can use the device camera to scan the registration sticker or operator sticker to obtain the details of the vehicle and its registered owner. This will reduce the risk of human error on input.
63. Person, vehicle and organisation queries are utilised based on input information to return further details. These provide the Officer further information that they can utilise to ensure they have the correct item prior to including the details in their paperwork.
64. If the Officer does not utilise a direct lookup of the object they are still able to complete a search. The search results are returned in likelihood order. The Officer is required to select the item they think is the best match. The Officer is then provided further information that they can utilise to ensure they have the correct item prior to including the details in their paperwork.

R03. There is a privacy risk that the incorrect item is selected when searching for a person or vehicle.

65. The Officer is meant to confirm the individual's address prior to using the details in their paperwork as they could have a different address to the one that is stored in NIA. The Officer is prompted to ensure this occurs. However, there is the potential that the address is not updated.

R04. There is a privacy risk that the information input is not updated based on current information.

66. If an unknown person or vehicle is included in any TCR, family harm investigation or noting, the paperwork is passed to FMC who complete further lookups to try and identify any possible matches before creating a new record for the item.

Use and Disclosure

67. Information including within OnDuty is used to fulfil Police obligations under the Policing Act 2008 and the Land Transport Act 1998.
68. All information contained within the non-production versions of NIA is sourced from production. Therefore, when testing is completed on OnDuty production information has to be utilised to enable records to be matched and updated in the non-production version of NIA. Individuals are potentially unaware of this secondary usage of their information.

R05. There is a privacy risk that production information is utilised in non-production versions of OnDuty.

69. Information input into OnDuty may be shared with

- Police Infringement Bureau
- NZTA
- NZ Post
- Integrated Safety Response (ISR) agencies.

The introduction of OnDuty has not altered the previous information sharing provisions.

70. Individuals may not realise or expect that information about them will be disclosed to another agency. This is most likely in relation to Family Harm Investigations. The information sharing provisions regarding Family Harm Investigations are documented in the Information sharing guidelines- family harm.

Unique Identifiers

71. OnDuty does not assign any unique identifiers to individuals.
72. However, information collected from individual's may include their drivers licence number which is a unique identifier assigned by NZTA. The drivers licence number is disclosed to enable Police to identify the licence relating to the individual. This is the purpose it was assigned for.

G. Management Approach

Information Sharing

R01. There is a privacy risk that individuals are not well enough informed that their information will be shared with other agencies as a result of Family Harm Investigations.

73. People who provide their information to Police as part of a Family Harm Investigation may be unaware that it is going to be shared with multiple agencies including a number of NGOs. This information is provided at a stressful time with the individual's consent therefore it is important that they understand thoroughly how it will be used and shared to enable them to provide informed consent.
74. Currently the Officer will discuss information sharing with the individual. There is not currently a formal script for the Officer to follow and there is no evidence it has occurred although all information is affirmed by the Officer. There is a screen within the OnDuty application reminding the Officer to provide the information. Therefore, if contested it would be hard to prove it occurred.
75. There are plans to issue information cards to families showing contacts for further support. These are still being developed. There is the opportunity to include the "notice" on the rear but these won't be ready in time for the launch.

Use of Information in Non-Production Environments

R02. There is a privacy risk that information relating to individuals is not appropriately secured within non-production environments.

R05. There is a privacy risk that production information is utilised in non-production versions of OnDuty.

76. Information is used without consent of the individual within the non-production environment of OnDuty. This is a secondary usage of the information. This issue is further compounded as most of the information was collected for legislative requirements rather than consent.
77. The security of the information within the non-production environment is also unknown which increases the potential risk of a breach of the information if controls are not functioning correctly.

Accuracy

R03. There is a privacy risk that the incorrect item is selected when searching for a person or vehicle.

R04. There is a privacy risk that the information input is not updated based on current information.

78. Ideally when looking up a person the source of the information should be a piece of official identification. This allows the Officer to ensure that they have the correct information. There is still the opportunity for human error if the Officer is not able to scan in the details.
79. The Officer is provided with a list of possible matches based on the information they have searched, and they are able to view further information regarding the individual. This includes items such as photographs. Therefore, the risk of the person's details not being correctly identified is low if they currently exist within NIA.
80. However, if the person information is not currently located within NIA there is the potential that they are entered incorrectly. This is mitigated by all new people being double checked by the FMC prior to inclusion in NIA to ensure a match cannot be located. FMC also check all new vehicles entered into the system also.
81. When information is queried and used within an ION or WTW, the Officer is prompted to check the individual's address with them. This is particularly important as these will be sent to NZ Post to post paperwork to the individual. If the address is incorrect the individual will not receive their fines and / or requests to attend court.

H. Required Privacy Controls

82. It is recommended that the following privacy enhancing controls are designed and implemented.

Reference	Recommendation	Due Date
A01	Issue some guidance / script to officers about what they need to advise families regarding information sharing when creating a Family Harm Investigation.	Prior to Launch
A02	Include notes on the OnDuty application about what should be included in the discussion about information sharing and have officers confirm it was delivered.	July 2018
A03	Longer term when the new cards are developed it is recommended the privacy notice should be included on the back of the cards and a step included in the application to remind the Officer to provide a card to the family.	August 2018
A04	Update all privacy notices to include the usage of production information in non-production environments.	May 2018
A05	Complete a C&A for the non-production environments of OnDuty.	June 2018