

15 January 2025

Alex

[fyi-request-29236-9e585c47@requests.fyi.org.nz](mailto:fyi-request-29236-9e585c47@requests.fyi.org.nz)

Tēnā koe Alex

### ***Request for information***

Thank you for your Official Information Act 1982 (OIA) request of 18 November 2024. You requested:

*I would like to know which specific information held about individuals by the New Zealand police has been shared with Research NZ, i.e. first name, last name, cellphone, etc. I would like to know whether this complies with the information stated here: <https://www.police.govt.nz/about-us/privacy-statement-how-we-manage-personal-information>.*

*I would like copies of the agreement between the NZ Police and Research NZ detailing how this information is stored and secured by research NZ and the requirements they have agreed to relating to this information.*

*I would also like to understand whether the information given by NZ Police to Research NZ is included in personal information requests by individuals to the NZ Police and if corrections to this information are forwarded to and corrected by Research NZ.*

New Zealand Police (Police) contracted Rangahau Aotearoa | Research New Zealand as a third-party agency to undertake a customer experience research programme. The main component of the programme is a survey named *Our Service, Your Say* | *Ō Whakaaro, Ā Mātou Mahi* (or OSYS for short). <https://www.police.govt.nz/about-us/publication/nz-police-our-service-your-say>

OSYS survey participants are sourced from one of two places: Police and Dynata (a panel provider). For the Police sample, Police securely provides Rangahau Aotearoa | Research New Zealand with monthly samples of information of selected people who have phoned the 105 service or reported an incident or crime to 105 online in the previous month.

For the purposes of the OSYS survey Police does not share with Rangahau Aotearoa | Research New Zealand any personal information about any person aged under 16 years or any person who has been involved in certain types of incidents (including homicide, aggravated robbery, sexual assault, domestic violence, suicide, child abuse and other offence types).

The individual level information Police shares with Rangahau Aotearoa | Research New Zealand for the purpose of the OSYS survey for the monthly 105 call samples is limited to:

- first and family name
- preferred email address

- preferred telephone number
- District within which the incident/occurrence took place
- station boundary within which the incident/occurrence took place
- SR.CRIS# (service request number and database used)
- acceptance date

And the equivalent information Police shares for the monthly 105 online samples is limited to:

- first and family name
- email address
- telephone number
- District within which the incident/occurrence took place
- station boundary within which the incident/occurrence took place
- case ID
- case creation date
- preferred contact method.

The privacy practices for the OSYS survey comply with information on the Police website at: <https://www.police.govt.nz/about-us/privacy-statement-how-we-manage-personal-information>.

All aspects of the OSYS survey are conducted in accordance with the provisions of the Privacy Act 2020 with respect to confidentiality, and methods of obtaining, storing, and destroying information.

The Consultancy Services Order (CSO) between Police and Research NZ provides for the secure protection and destruction of information related to the OSYS survey.

Clause 10 Confidentiality of Part F of the Terms of the CSO covers how personal information will be kept confidential. Please refer to the appendix for the full text of Clause 10, in accordance with section 16(1)(e) of the OIA.

Other relevant extracts from the CSO are set out below:

Research NZ will ensure on an annual basis that an independent data security compliance and assurance review and written confirmation to NZISM standard will be provided to Police on the contract anniversary each year.

Research NZ will not electronically store any Police research data offshore unless this has been prior agreed with Police and confirmed by Police in writing.

Research NZ will only permit those personnel who have been vetted and approved by Police in accordance with the Police security checking system to be involved in any way dealing with the Services.

In addition to Part F clause 14.2 c any Police Documentation or Data files returned to Police must be in a readable and usable format. Any copies of Documentation or Data Files retained by Research NZ will then be destroyed and confirmed to Police.

I also attach a Privacy Impact Assessment undertaken by Rangahau Aotearoa | Research New Zealand specifically for the OSYS survey.

The monthly sample sets that Police shares with Rangahau Aotearoa | Research New Zealand for the purposes of the OSYS survey are used once by Rangahau Aotearoa | Research New Zealand. Rangahau Aotearoa | Research New Zealand deletes these sample sets after six months.

You have the right to seek an investigation and review by the Ombudsman of this decision. Information about how to make a complaint is available at [www.ombudsman.parliament.nz](http://www.ombudsman.parliament.nz) or freephone 0800 802 602.

Nāku noa, nā



Susan Campbell  
Principal Advisor Service Strategy  
New Zealand Police

## Appendix: Clause 10 Confidentiality of Part F of the Terms of the CSO

### 10. Confidentiality

#### 10.1 Protection of Confidential Information

- (a) Subject to clauses 10.1(c) and 10.2, the Provider and the Participating Agency will treat as confidential and not disclose to any third party nor use for its own benefit any Confidential Information that is the Confidential Information of the other.
- (b) The Provider will:
  - (i) ensure that all Confidential Information of the Participating Agency (and any backup archives containing such Confidential Information) in the possession or control of the Provider from time to time is kept secure and managed and protected and only disclosed or otherwise dealt with in accordance with this Consultancy Services Order;
  - (ii) not use any Agency Information for its own purposes or for any purposes different from those contemplated by this Consultancy Services Order; and
  - (iii) advise the CoE in writing if any Confidential Information of the Participating Agency will be transferred or stored outside New Zealand before such information is transferred and will confirm that the requirements of this clause 10.1 will be met while such Confidential Information is stored outside New Zealand.
- (c) Clause 10.1(a) does not prevent the disclosure of Confidential Information:
  - (i) if that information was known, or becomes known, to the public through no act or default of the recipient;
  - (ii) that the recipient is required by Law or parliamentary practice (including parliamentary questions) to disclose, or to a Select Committee or to a Minister of the Crown, so long as the recipient provides notice of the required disclosure promptly upon receipt of notice of the required disclosure (if it is permitted to do so by Law);
  - (iii) that was lawfully known to the recipient prior to the date it was received;
  - (iv) that becomes available to the recipient from a source other than a party to this Consultancy Services Order, provided that the recipient has no reason to believe such source is itself bound by an obligation of confidence to the person that disclosed that information or is otherwise prohibited under Law from disclosing such information;
  - (v) to any Professional Adviser for the purposes of rendering professional services to a party in relation to this Consultancy Services Order;
  - (vi) to the extent that such disclosure is authorised by this Consultancy Services Order; or
  - (vii) if such disclosure is approved for release with the consent of the party from whom the Confidential Information is first received.

#### 10.2 Limited disclosure

- (a) The Provider may, subject to clause 10.2(d), disclose the Confidential Information of the Participating Agency to its Subcontractors, Personnel, Related Entities and Professional Advisers who need to know the same



for the sole purpose of enabling the Provider to perform its obligations and exercise its rights under this Consultancy Services Order.

- (b) The Participating Agency may, subject to clause 10.2(d), disclose the Confidential Information of the Provider to its third party suppliers, Personnel and Professional Advisers and any other Participating Agencies (including the CoE) who need to know the same in connection with the Services.
- (c) The Provider will not disclose the Participating Agency's Confidential Information to any of its Subcontractors, Related Entities or Professional Advisers, and the Participating Agency will not disclose the Provider's Confidential Information to any of its third party suppliers or Professional Advisers, unless the recipient has given a written confidentiality undertaking to the disclosing party in terms substantially similar to those set out in this clause 10.
- (d) Any undertaking given pursuant to clause 10.2(c) will be provided to the other party to this Consultancy Services Order on request.

## MEMORANDUM | 11 AUGUST 2023

**To** Susan Campbell and Judy Paulin, Ngā Pirihimana o Aotearoa/New Zealand Police

**From** Emanuel Kalafatelis, Melissa Lotter and Katrina Magill  
Rangahau Aotearoa Research New Zealand

**Subject** Our Service, Your Say (OSYS) (#5278)

### Project summary

Rangahau Aotearoa (Research New Zealand) is responsible for Ngā Pirihimana o Aotearoa's Customer Experience Research Programme via the Our Service, Your Say survey (OSYS).

The purpose of this research is to:

1. Measure New Zealanders' satisfaction with the contact and interaction they have had with Ngā Pirihimana o Aotearoa (for KPI reporting).
2. Identify areas for potential service improvement.

The research involves the completion of online questionnaires and telephone (CATI) interviews with approx. n=8,000 New Zealanders who have had recent contact with Ngā Pirihimana o Aotearoa (i.e. in the last 6 months). Māori, Pasifika, people aged 16-24 and those living in Tāmaki Makaurau are over-sampled.

Respondents are currently sampled from two sources:

1. Directly via 105 (phone and online reporting)
2. Indirectly via our online provider (Dynata).

All survey respondents participate on a voluntary, confidential basis. The core set of questionnaires are based on the Common Measurements Tool and includes a specifically designed module of questions for Māori respondents, as well as a module containing hate crime questions.

Reporting is in multiple forms:

1. An online e-reporting tool.
2. A publicly available annual report (on Ngā Pirihimana o Aotearoa's website).



## Scope of this Privacy Impact Assessment

This PIA covers the following processes:

1. Obtaining samples of potential respondents.
2. Recruiting respondents based on the survey eligibility criteria.
3. Completing confidential survey about the contact with Ngā Pirihiimana o Aotearoa.
4. Processing and reporting the survey results back to Ngā Pirihiimana o Aotearoa.
5. Saving and storing the survey information.
6. System-level reporting.

These processes require the use of the following systems and tools:

- Microsoft Teams (used to receive 105 samples from Ngā Pirihiimana o Aotearoa).
- Voxco (survey tool).
- MS SQL server.
- Bespoke online e-reporting tool.

## Information security management strategy

Rangahau Aotearoa has an **information security management strategy** which sets out the high-level context for managing information resources required for the purposes of conducting research projects. This is built on the New Zealand Privacy Act 2020, the government's New Zealand Information Security Manual (v 3.6), the European Union's General Data Protection Guidelines and our Code of Practice (i.e., the Code of the European Society for Marketing & Opinion Research).

At the heart of this strategy are **four principles** that underpin how information resources are to be used:

1. **Information is an asset** – information should be treated as an asset, managed, and used to realise its full potential for Rangahau Aotearoa's clients.
2. **Information provides insight** – information supports the work that Rangahau Aotearoa completes on behalf of its clients.
3. **Information is well-managed** – information should be kept secure, managed efficiently and effectively, as well as ethically at all times.
4. **Information is protected** – information should be utilised unless there are grounds for refusal, such as for confidential and/or personal reasons.

These principles are built into our functional/operational practices, and it is important that everyone (Ngā Pirihiimana o Aotearoa and Rangahau Aotearoa) is aware of their responsibilities with respect to managing information appropriately. These practices cover:

- How we obtain personal information (Data transfer).
- How we handle this information (Access management).
- Survey implementation and support.
- Confidentiality (Depersonalisation).
- Our approach to analysis and reporting, including the online e-reporting tool.
- Our approach to counter security attacks (Penetration testing).
- Physical security.
- Data storage, recovery, and restoration.

### **Data transfer**

As noted, potential respondents for OSYS are sourced via Ngā Pirihiimana o Aotearoa's 105 (online and telephone) and our panel provider (70% and 30% respectively).

There is no transfer of personal information about potential respondents sourced via our panel provider. In the case of personal information about potential respondents sourced via Ngā Pirihiimana o Aotearoa's 105 (see Table 1, 1 for details), a monthly sample is received via Ngā Pirihiimana o Aotearoa's SFTP server, minus exclusions. The exclusions include anyone under 16 years of age, Police staff and anyone whose contact with Ngā Pirihiimana o Aotearoa was related to a serious matter or one that might put the respondent at risk of harm (refer to Appendix A).

### **Access management**

On receipt of the 105 monthly samples from Ngā Pirihiimana o Aotearoa, they are saved in a specific project folder, with access to this folder restricted to those staff directly working on the project. This is actively monitored by our IT Manager.

In preparation for contacting potential respondents, the samples are 'cleaned', which in addition to re-formatting, involves checking for incomplete contact details and excluding anyone who has already been sampled within the previous six months or who has contacted us to request that they not be approached for any future research.

At the same time in the monthly cycle, potential respondents are then contacted, introduced to the survey and their eligibility to complete it established. As part of this step, potential respondents are told that the survey is voluntary, confidential and they will not be directly or indirectly identifiable in the results.

Please note that our sample and data security practices meet and exceed the requirements of the government's New Zealand Security Manual (v 3.6).



## Survey implementation

All eligible respondents sampled via our panel provider complete the survey online. Eligible respondents sampled via Ngā Pirihiimana o Aotearoa's 105, are given the option of completing the survey online or by telephone. The survey is available in te reo Māori, Samoan, Tongan and simplified Chinese.

Please note that our online survey platform (Voxco) is SSL and SOC2 certified. It also has the features expected of a modern survey platform in terms of accessibility, in that it already meets WCAG 2.1 AA and is expected to meet WCAG 2.2 AA when this is available later this year.

Our survey platform is a fully supported system with assistance provided within a same-day timeframe. Our purpose-built, CATI-enabled Call Centre telephone (which is also based on the Voxco survey platform) operates in conformance with ISO 20252. All telephone interviews are audio recorded (with respondents' consent) and our Call Centre Manager and her Supervisors complete quality assurance checks with a random selection of every interviewer's successful and unsuccessful interviews (5 per month for each interviewer).

## Depersonalisation

As noted above, all respondents participate in the survey on a voluntary, confidential basis, meaning that at no time does Ngā Pirihiimana o Aotearoa know which individuals have participated in the survey and which have not.

With respect to the sample sourced via Ngā Pirihiimana o Aotearoa's 105, any personally identifiable information is removed as part of the processing process post-interviewing. This includes information in any verbatim comments such as names, places, events, and reference to time. This also applies to the sample sourced via our panel provider.

## Analysis and reporting

All analysis and all reporting is completed on an aggregated basis; meaning that no individual respondent is either directly or indirectly identifiable in any reporting.

## Online e-reporting tool

A bespoke online e-reporting tool has been built for the purposes of sharing the survey results with Ngā Pirihiimana o Aotearoa.

This online e-reporting tool was built in-house and is on an SSL-enabled website with 256-bit encryption. This means that it is only accessible via a username and password, set to the minimum NZISM requirements.

Susan Campbell, Principal Advisor Service Strategy, Ngā Pirihiimana o Aotearoa, is primarily responsible for authorising and removing Police users with access to the e-reporting tool, which is hosted on Rangahau Aotearoa's digital platform. Vicky Jamieson, National Channel Lead - Front Counter, will assume responsibility for this in Susan's absence.

Access to the e-reporting tool by authorised Police users is by logins (using their QID) and passwords (randomly generated weekly by Rangahau Aotearoa and the same for everyone).

Susan (supported by Vicky) maintains a file containing a list of QIDs that are sent to Rangahau Aotearoa of those Police people she authorises access to the survey results through the e-reporting tool.

Rangahau Aotearoa completes the following steps **each** week:

- Step 1: Randomly generates one password for all Police users.
- Step 2: Uploads the file of QID and sends an email to all Police users letting them know the password.

Susan (supported by Vicky) reviews the file of QIDs on the first working day of each month and emails a revised file (with those of new Police people, etc.) to Rangahau Aotearoa.

Police users who move roles within Police are able to continue to access the survey results through the e-reporting tool. Those who resign (and whose QIDs are cancelled) are not able to access the e-reporting tool once the password changes.

The *Our Service, Your Say* survey results are only accessible to authorised Police users in aggregate form (in line with undertakings of confidentiality with survey participants). Survey results are shown in the tool for sub-samples comprising 10 survey participants or fewer, and all personally identifiable information is deleted from verbatims before they are made accessible through the e-reporting tool.

### **Penetration testing**

Rangahau Aotearoa Research New Zealand conducts scheduled penetration testing on an annual basis. This is completed by an independent third party (viz. Aura). Testing is scheduled for November each year.

### **Physical security**

Rangahau Aotearoa Research New Zealand is in downtown Wellington CBD (Level 6, 22 Panama Street), in fully secure offices.

### **Data storage**

All project-related files are saved and stored in the cloud, in a depersonalised format, with our government-approved local cloud provider, CCL. All data is stored onshore.

## Privacy assessment

The following table provides a privacy assessment for Ngā Pirihiimana o Aotearoa’s OSYS, against the 13 privacy principles (as per the New Zealand Privacy Commissioner).

**Table 1: Privacy assessment**

	Description of privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
1	<p>Principle 1 – Purpose of the collection of personal information.</p> <p><b>Be focused – only collect personal information if you really need it.</b></p>	<p>Limited personal ‘primary’ information is provided by Ngā Pirihiimana o Aotearoa for the purposes of contacting potential 105 respondents and/or analysing and/or reporting their survey results.</p> <ul style="list-style-type: none"> <li>• Their first and family name.</li> <li>• Their email address and telephone contact number.</li> <li>• The Police District in which the most recent incident reported, took place.</li> </ul> <p>This information is saved in the project-specific folder for OSYS; access to which is restricted and actively monitored by our IT Manager.</p> <p>As noted, no personal information is provided for our panel provider-sourced sample. However, survey questions are asked to establish all respondents’ gender, age and ethnicity (personal ‘secondary’ information). They are also asked about the purpose of their contact with Ngā Pirihiimana o Aotearoa.</p> <p>Any personal ‘primary’ or ‘secondary’ information, which is capable of directly identifying a respondent (e.g. name, phone number, etc) is limited in its use and removed/separated from the survey results after collection (see below, Principle 4).</p>	Compliance met.

2	<p>Principle 2 – Source of personal information.</p> <p><b>Be direct – get it directly from the people concerned wherever possible.</b></p>	<p>Refer above.</p> <p>To ensure respondents are comfortable providing personal information, as part of the recruitment process, they are told that the survey is voluntary (as are providing answers to the survey questions).</p> <p>During the interview, they can withdraw at any time. Post-interviewing, they can ask for a transcript of their interview and/or their interview to be deleted.</p> <p>On multiple occasions, they are told that their responses are confidential to Rangahau Aotearoa and that all reporting to Ngā Pirihiimana o Aotearoa is on an anonymous basis as required by our Code of Practice, Privacy Act 202, etc.</p>	Compliance met.
3	<p>Principle 3 – Collection of information from the individual.</p> <p><b>Be open – tell people 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.</b></p>	<p>Refer above.</p> <p>Email invitations to complete the survey explain the purpose of the survey, that participation is voluntary, respondents remain anonymous and that reporting is in an aggregated, summary form.</p> <p>The same information is available to respondents interviewed by telephone and is provided by our interviewers on request.</p>	Compliance met.
4	<p>Principle 4 – Manner of collection of personal information.</p> <p><b>Be considerate, be fair and don’t be overly intrusive in how you collect the information.</b></p>	<p>The survey is implemented (online or by telephone) via Rangahau Aotearoa New Zealand’s secure online survey panel.</p> <p>As soon as completed surveys are processed, any personally identifiable primary information (name and contact details) is removed/separated from the survey results.</p> <p>This includes verbatim comments provided to any free text, open-ended questions.</p>	Compliance met.

5	<p>Principle 5 – Storage and security of personal information.</p> <p><b>Take care of it once you’ve got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.</b></p>	<p>The monthly Ngā Pirihi mana o Aotearoa-sourced 105 samples containing personal information are stored on Rangahau Aotearoa Research New Zealand’s Voxco survey platform.</p> <p>Following the completion of each month’s surveying, the survey data is extracted, depersonalised (see above, Principle 4), checked for outliers, coded, weighted and uploaded to the online e-reporting tool.</p> <p>In addition to the above, our Data Security Policies and Practices detail a number of safeguards to ensure information is well managed. These include:</p> <ul style="list-style-type: none"> <li>• how files containing personal identifiable information are handled</li> <li>• access control</li> <li>• data storage and protection</li> <li>• device and physical security</li> <li>• recovery and restoration.</li> </ul>	Compliance met.
6	<p>Principle 6 – Access to personal information.</p> <p><b>Keep people informed – tell them what personal information you hold.</b></p>	<p>Under Rangahau Aotearoa Research New Zealand’s Code of Practice, respondents may request to see their survey responses after it has been captured/submitted. If such a request is made, they are provided a hard/soft copy of the survey questionnaire showing their responses.</p>	Compliance met.
7	<p>Principle 7 – Correction of personal information.</p> <p><b>Make it right – let them correct it if you have got it wrong.</b></p>	<p>Also, in accordance with the Code, respondents may also change their response to a question(s) after it has been captured/submitted.</p> <p>On request, they are provided the OSYS project manager’s name and contact details for this and other purposes (e.g. if they are having technical difficulties).</p>	Compliance met.

8	<p>Principle 8 – Accuracy of personal information is to be checked before use.</p> <p><b>Keep on the mark – ensure its correct and relevant before you use it.</b></p>	<p>There is an expectation that the personal information provided by respondents at the time of recruitment (e.g. about their eligibility to complete the survey) and during their interview (e.g. age, gender, ethnicity) is <u>correct</u>. This is also the case with the information provided by Ngā Pirihiimana o Aotearoa with respect to the 105 samples.</p> <p>Respondents’ answers to the questions in the survey are also taken at face value and assumed to be correct, subject to the removal of outliers.</p>	Compliance met.
9	<p>Principle 9 – Not to keep personal information for longer than necessary.</p> <p><b>Don’t be a hoarder – get rid of it if you don’t need it anymore.</b></p>	<p>As noted above (see above, Principle 4), completed surveys are checked post-interviewing before any personally identifiable primary information is removed/separated from the survey results. This process is completed within one week of the interviewing having been completed.</p> <p>This means that when this information has been removed, each interview is completely anonymous.</p>	Compliance met.
10	<p>Principle 10 – Limits on use of personal information.</p> <p><b>Stick to the plan – only use it for the purpose you initially collected it for.</b></p>	<p>Rangahau Aotearoa Research New Zealand confirms that the personal information that is provided by Ngā Pirihiimana o Aotearoa and/or collected during the interviewing is only used for the purposes intended (see <i>Project Summary</i> at the beginning of this paper).</p>	Compliance met.
11	<p>Principle 11 – Limits on disclosure of personal information.</p> <p><b>Keep the control – only share information if that’s why you got it.</b></p>	<p>Not applicable. i.e., Rangahau Aotearoa will never disclosed personal information obtained of people in 105 samples, or through the survey itself.</p>	Not applicable.
12	<p>Principle 12 – External disclosure.</p> <p><b>Only disclose personal information outside NZ if the receiving organisation has comparable privacy safeguards to NZ.</b></p>	Not applicable.	Not applicable.

13	<p>Principle 13 – Unique identifiers.</p> <p><b>Be unique – don’t use other agencies’ personal identifiers.</b></p>	<p>Rangahau Aotearoa assigns unique identifiers to each respondent as they onboard OSYS.</p> <p>These are primarily used for project management purposes (e.g., to track the response to the survey).</p>	Compliance met.
----	---	---	-----------------



## Risk assessment

The following table provides a risk assessment for OSYS.

**Table 2: Risk assessment**

Risk	Risk assessment	Mitigation	Category
Use of Ngā Pirihiimana o Aotearoa-sourced 105 sample information.	Low	Limited contact information is provided by Ngā Pirihiimana o Aotearoa and this is only used to recruit potential respondents and/or analysing and/or reporting their survey results. Access to this information is restricted and primary information (name and contact details) is deleted/separated from the survey results post-interviewing, before the survey results are analysed and reported.	Process.
Capture of personal information as part of the recruitment/interviewing process.	Low	Aside from high-level demographic information and information about the reason for contact with Ngā Pirihiimana o Aotearoa, no other information which may be categorised as personal 'primary' information' is collected.  As noted, survey results are depersonalised as soon as practically possible, by removing/separating the personal 'primary' information.	Process.
Access protocols for Rangahau Aotearoa Research New Zealand users that have access to the Ngā Pirihiimana o Aotearoa-provided samples and survey data in general.	Low	These protocols need to be established in order to set out the terms and conditions for the use of this information.	Process.
Access protocols for Ngā Pirihiimana o Aotearoa users that have access to the survey data via the online e-reporting tool (including how Ngā Pirihiimana o Aotearoa users' agreement will be obtained).	Low	Access to the e-reporting tool by Ngā Pirihiimana o Aotearoa staff is controlled through use of a current Police user id (approved by Susan Campbell) and a password changed and communicated weekly to these staff by Rangahau Aotearoa.	Process.

## Action plan

The following table outlines the actions that will be taken to mitigate the identified risks for the OSYS.

**Table 3: Action plan**

	<b>Action</b>	<b>Responsibility</b>	<b>Date of completion</b>
1	Review method of use of Ngā Pirihiimana o Aotearoa-sourced 105 sample information.	Katrina Magill/Sarah Buchanan.	Monday 29 January 2024
2	Review method of capturing personal information via the recruitment/interviewing process.	Katrina Magill/Sarah Buchanan.	Monday 29 January 2024
3	Establish and record project folder and access permissions.	Katrina Magill/Sarah Buchanan.	Monday 29 January 2024
4	Prepare T&Cs for the removal of personally identifiable information.	Katrina Magill/Sarah Buchanan.	Monday 29 January 2024
5	Prepare T&Cs for access permissions for Ngā Pirihiimana o Aotearoa users to access the online e-reporting tool.	Katrina Magill/Sarah Buchanan.	Monday 29 January 2024

## Appendix A – Exemptions

**Table 4: 105 Call Sample Exclusions**

Code	Incident/Offence
1110	Murder
1210	Kidnapping
1310	Aggravated Robbery
1410	Wounding With Intent
1510	Aggravated Assaults
1640	Common Assault
1D	Domestic Dispute
1E	Emergency/Disaster/Spill
1F	Assist Fire/Ambulance/Traffic
1S	Sudden Death
1X	Threatens/Attempts Suicide
2210	Indecent Performance And Acts
2510	Video Recordings Act 1987
2610	Abduction for Sex
2630	Indecent Assaults
2650	Sexual Violation
2710	Incest
2810	Unlawful Sexual Intercourse
2910	Brothels And Prostitution
2A	Advise Relatives
2T	Warrant To Arrest/Fines Enforcement
2U	Warrant of Seizure
2W	Warrant to Arrest
2Z	Other Service Request Response
3710	Child Abuse (Not Assault)
3850	Domestic Violence Act 1995
3M	Directed Patrol
3R	Road Check
3V	Staff Visit/Supervision
4410	Receiving/possessing Stolen Goods
4B	Mortuary Procedure
4F	Forensic Examination
4G	Travel
4H	Photography Job
4L	Logistics/Staff Transport
4Q	Enquiry/Investigation
4X	Execute Search Warrant
5F	Family Harm Investigation
5K	Bail Check
6D	Bail Breach

Code	Incident/Offence
6E	EM Bail Breach
6S	Police Safety Order Breach
7120	Offences Against Judicial Procedure
7130	Offences After Sentence Passed
7420	Criminal Investigation (blood Smples) 1995
7610	By Laws Prosecuted By Police

**Table 5: 105 Online Sample Exclusions**

Code	Incident/Offence
1000	Violence
1100	Homicide
1200	Kidnapping and Abduction
1300	Robbery
1400	Grievous Assaults
1500	Serious Assaults
1600	Minor Assaults
2000	Sexual
2100	Sexual Attacks
2200	Sexual Affronts
2300	Abnormal Sexual Relationships
2400	Immoral Behaviour
2500	Indecent Videos
2600	Sexual Attacks
2700	Abnormal Sex
2800	Immoral Behaviour
2900	Immoral Behaviour/Miscellaneous
1D	Domestic Dispute
1E	Emergency/Disaster/Spill
1F	Assist Fire/Ambulance/Traffic
1S	Sudden Death
2A	Advise Relatives
2T	Warrant To Arrest/Fines Enforcement
2U	Warrant of Seizure
2W	Warrant to Arrest
2Z	Other Service Request Response
3M	Directed Patrol
3R	Road Check
3W	Watching/Observations
5F	Family Harm Investigation
5K	Bail Check

Code	Incident/Offence
3710	Child Abuse (Not Assault)
3850	Domestic Violence Act 1995
4110	Burglary For Drugs
7120	Offences Against Judicial Procedure
7130	Offences After Sentence Passed
7140	Miscellaneous Offences Against Justice
7160	Other Breaches Miscellaneous Statute

Case Crime Type: CHILD ABUSE;HOMICIDE;OTHER SEXUAL VIOLATIONS;SEXUAL VIOLATIONS;SUDDEN DEATH;FAMILY INCIDENT;FAMILY VIOLENCE;GRIEVOUS ASSAULT;SERIOUS ASSAULT

File Type: V - Family Violence