

DIRECTIONS AND DELEGATIONS

Sections 17 and 95C Policing Act

Delegated/authorised employees who may disclose information under section 95B of the Policing Act:

- **under an international disclosure instrument; or**
- **in accordance with these Directions**

Pursuant to sections 17 and 95C of the Policing Act 2008 (the Act), I, Tania Kura, Commissioner of Police, give the Police employees described below:

- delegated authority to exercise the Commissioner's powers, functions and duties to disclose information under section 95B of the Policing Act 2008 (the Act) whether in accordance with an international disclosure instrument or in accordance with my directions; and
- authorisation in accordance with section 95C(2) of the Act and these Directions to disclose personal information held by Police to a corresponding overseas agency outside of an international disclosure instrument.

Those employees are:

1. Employees holding the following levels of position or acting at that level of position:
 - 1.1 Deputy Commissioner
 - 1.2 Assistant Commissioner
 - 1.3 Deputy Chief Executive
 - 1.4 Executive Director
 - 1.5 Chief Financial Officer
2. All employees belonging to the following work groups:
 - 2.1 International Services Group
 - 2.2 Police Vetting Service
 - 2.3 Financial Crime Group
 - 2.4 National Security Group
3. Employees appointed to or from time to time acting in the following roles:
 - 3.1 Shift Commanders in Police Communications Centres
 - 3.2 Director Emergency Communication Centres
 - 3.3 National Operations Manager Emergency Communications
 - 3.4 Director Integrity and Conduct
 - 3.5 Operations Manager, Police Professional Conduct, Integrity and Conduct
 - 3.6 Deployment Manager, Integrity and Conduct
 - 3.7 Manager: National Command and Coordination Centre
 - 3.8 Shift Commanders and Shift Coordinators in the National Command and Coordination Centre
4. Employees in:
 - 4.1 the National Organised Crime Group and who hold the level of position of Detective Sergeant or above.
 - 4.2 the National Organised Crime Group Intelligence Team

5. Employees in:
 - 5.1 the Cybercrime Unit who hold the level of position of Sergeant or above
 - 5.1 the Cybercrime Intelligence Team
 - 5.2 the COLT who hold the level of position of Sergeant or above
 - 5.3 the COLT Intelligence team
 - 5.4 the OCEANZ Victim Identification team
- 6 Employees in the National Criminal Investigations Group holding the level of position of Detective Sergeant or above (or Police employee equivalent).
- 7 The following National Intelligence Centre employees:
 - 7.1 Employees in the National Intelligence Centre who are supervisors and above
 - 7.2 Employees in the National Intelligence Centre Registry
 - 7.3 NIC International Intelligence Officer, Canberra
- 8 Constabulary investigators who:
 - 8.1 Are working on an investigation or operation involving a corresponding overseas agency that is being coordinated by INTERPOL Wellington; and
 - 8.2 Have been directed by INTERPOL Wellington to correspond directly with a corresponding overseas agency in relation to the specific investigation or operation

provided those investigators communicate with that corresponding overseas agency about the investigation or operation in a way that INTERPOL Wellington is able to continue to oversee those communications (for example, by copying INTERPOL Wellington in on emails).
- 9 Employees in the following roles in the Firearms Safety Authority / Te Tari Pūreke:
 - 9.1 Constabulary employees at the level of position of Inspector or above
 - 9.2 Regional managers
 - 9.3 Firearms Registry managers
 - 9.4 Compliance managers
 - 9.5 Resolutions managers
- 10 Employees in Protection Services at the level position of Senior Constable and above

For the purposes of this delegation and authorisation, where a work group or employee role is listed above, that shall also include any other name that the above-listed work group or role may subsequently be known by.

Further directions to authorised employees for sharing information outside of an international disclosure instrument

In addition, I make the following further directions under section 95C of the Policing Act which apply to those employees above who are authorised to disclose personal information held by Police to a corresponding overseas agency outside of an international disclosure instrument in accordance with section 95B(3)(b).

Authorised employees may share personal information in accordance with section 95B(3)(b) of the Policing Act where:

- the proposed disclosure would be to a “corresponding overseas agency” (or someone authorised to act on the agency’s behalf); and
- the disclosure of personal information is reasonably necessary to enable the corresponding overseas agency to perform a function in its jurisdiction that Police perform in New Zealand under section 9 of the Policing Act; and
- the proposed disclosure would be in accordance with these Directions.

Authorised employees may only disclose information that is “reasonably necessary” for the purposes stated and need to consider whether this requirement limits the amount or type of information that can be released.

When disclosing information under section 95B, authorised employees must ensure that the foreign agency that will be receiving the information is made aware that the information is being released by New Zealand on the following basis and the foreign agency will inform New Zealand Police in the event of a breach of those requirements. The information should be released on the basis that the information:

- will only be used for the purpose for which it has been sought/provided
- will be stored securely and then destroyed when it is no longer required
- will not be disclosed to a third party without written authorisation from New Zealand Police
- will not be used for the prosecution or punishment of a person for an offence in respect of which the person may be or has been sentenced to death unless such use has been approved in writing by the New Zealand Central Authority for mutual assistance, the Crown Law Office.

An employee who becomes aware that any of these conditions have been breached by the receiving agency must notify their supervisor and follow the process set out in the relevant Police policy for managing privacy breaches.

After disclosing personal information under section 95B (including any verbal disclosure), authorised employees must retain a record of the information disclosed and who the information was disclosed to. This should be done by emailing the information disclosed to PIRI@police.govt.nz (for example, by using the cc or bcc field). However, if there are operational imperatives that mean emailing the PIRI email address is not appropriate (for example, classified information is involved):

- the disclosing employee’s workgroup must:
 - a. ensure that the workgroup retains records of each of the workgroup’s disclosures under the Policing Act;
 - b. ensure that the Chief Privacy Officer is made aware that the workgroup will be retaining its international information sharing records (or particular category of them); and
 - c. collate and send those records by mid-February each year (to cover the period from January to December of the previous year) to the Chief Privacy Officer, Assurance Group; and

- the disclosing employee must keep records in accordance with their workgroup's processes.

The Chief Privacy Officer reports annually to the Privacy Commissioner on Police's use of this information sharing provision. To enable this, the Chief Privacy Officer needs to be able to review a sample of disclosures made. It is expected that most disclosures will be recorded in the PIRI mailbox through the above procedures, and any that are not, will be made available to the Chief Privacy Officer each year.

Dated at Wellington this 19th day of November 2024

A handwritten signature in dark ink, appearing to read 'Tania Kura', followed by a period.

Tania Kura
Commissioner of Police