

PRIVACY POLICY

1 BACKGROUND AND SUMMARY

The purpose of this policy is to provide clear guidelines on the collection, use, storage and disclosure of personal information and to ensure compliance with the [Privacy Act 2020](#) (the Act).

By following this policy, you will help protect POAL's reputation and its relationships with customers, suppliers and staff. Failure to follow this Policy may result in disciplinary action.

Rules around the collection, use, storage and disclosure of personal information by POAL are set out in thirteen Information Privacy Principles (IPPs) – for the detail see [Part 3 of the Act](#).

Personal information includes, but is not limited to:

- Information about an individual including name, gender, address, date of birth, contact details, employment history, driving licence or other relevant identity credential, salary and medical information;
- Personal details about staff, contractors, customers, suppliers and other contracting parties - including details of the directors, shareholders, representatives and employees of those organisations;
- CCTV footage of customers, employees, contractors suppliers and/or any other visitors to the Port; and
- Recording of radio communication channels.

2 SCOPE

This Policy covers all Directors, employees and contractors of Ports of Auckland Limited (POAL), and its subsidiaries.

3 PRIVACY OFFICER

POAL's Governance & Risk Manager is the [Privacy Officer](#) and is responsible for:

- encouraging compliance by POAL with the IPPs, including overseeing privacy awareness training;
- dealing with requests made to POAL under the Act;
- investigating, advising on, handling and monitoring any near misses, privacy breaches, or privacy complaints;
- working with the Privacy Commissioner in relation to investigations conducted into privacy complaints;
- reporting to the POAL Board on any privacy issues relating to POAL; and
- otherwise ensuring POAL's compliance with the Act.

If the Governance & Risk Manager is not available, then the [Alternate Privacy Officer](#) is the Governance and Risk Advisor.

4 COMPLAINTS / BREACHES

POAL will do all that it can to safeguard personal information. Any suspected or known breaches of Privacy will be investigated by the Privacy Officer, who will take action to prevent any further breach and minimise the impact.

Where the breach of personal privacy has the potential to cause embarrassment or harm, the affected individual will be advised of the breach and supported to minimise the impact, and POAL will seek to agree a remedy acceptable to the individual.

Should there be an accidental breach of Privacy, through carelessness, poor judgement or non-criminal negligence, POAL will take all possible means to rectify the error and minimise its impact in a timely way. Training will be provided to the person committing the breach to prevent any reoccurrence.

Should there be a deliberate breach of Privacy, the person in breach will be considered to have committed serious misconduct and may be subject to disciplinary procedures up to, and including, dismissal. In the case of Contractors, a deliberate breach may result in the cancellation of their contract.

If there is a notifiable breach (as defined in the Act) the Privacy Officer will notify the Privacy Commissioner as soon as practicable after becoming aware of the breach.

4.1 Complaint Process

To report a breach you will need to complete a [Privacy Complaint Form](#) and send it to the Privacy Officer.

The Privacy Officer will meet with you to discuss the [process](#) for dealing with your complaint.

You can make your complaint direct to the [Privacy Commissioner](#). The Commissioner will either investigate the complaint; or decide to take no action, following the rules set out in the Act. The Privacy Officer will assist the Privacy Commissioner in any investigation.

5 PRIVACY IMPACT ASSESSMENTS

For every project undertaken at POAL, the Project Manager will consider if there is any personal information involved. If so, the Project Manager will complete a [Brief Privacy Analysis](#) and discuss this with the Privacy Officer to ascertain whether a full Privacy Impact Assessment is required.

6 COLLECTION OF PERSONAL INFORMATION

Personal information will be collected only for a lawful purpose connected with and necessary for a POAL activity. Information will be collected directly from the individual concerned unless it is publicly available or the individual concerned authorises collection of the information from someone else.

The individual concerned must be aware of the fact that the information is being collected, the purpose for which the information is being collected, the intended recipients of the information and the rights of access to, and correction of, personal information.

Examples of personal information collected by POAL include, but are not limited to:

- Information sought on applications for employment
- Information required in order to pay employees or contractors

- Information required to contact next of kin in case of emergency
- Driving Licence or other relevant identity credential information
- Closed Circuit Television (CCTV) images
- Email and internet usage
- Information regarding access to the premises and movements around the Port (swipe card use).

7 CCTV SYSTEMS

POAL operates CCTV systems for the following purposes:

- The safety and security of staff, contractors, tenants, visitors to the Port and members of the public, including monitoring of operational activity on site;
- The security of POAL property, assets and cargo;
- To assist New Zealand Customs Service, Ministry of Primary Industries, New Zealand Police or any other Government agency in carrying out its duties.

7.1 Security / operational cameras

CCTV cameras are selected to ensure they are fit for purpose and the conditions of a 24/7 operational port. The majority of cameras covering the operational areas of the port are generally fixed to light towers providing wide coverage.

Cameras installed internally in buildings provide a broad view and are not fixed on individuals or their work areas unless there is no option. Where such a situation arises, modesty masking of the camera is undertaken.

Cameras along the perimeter are focused so as to capture footage along the fenceline without observing the outside public areas more than is absolutely necessary.

Cameras viewing the waterside are positioned to assist Harbour Control in the safe management of shipping operations. These cameras are located on light towers and provide a broad view.

Cameras are also used to monitor loads being placed on structures, identify the causes of damage to any port property or infrastructure, or to identify the causes of environmental spills or breaches.

7.2 Container handling equipment

Cameras are positioned in Container Handling Equipment (CHE) and give a wide view of the workspace. Footage may be used for health and safety purposes, training, monitoring of the use of equipment and monitoring of damage to equipment.

7.3 Awareness

Signs are erected in strategic locations in the vicinity of the CCTV cameras and along the perimeter fence of the CCTV system's range (before individuals enter the range of the cameras) to notify people that cameras are operating.

A [Privacy Notice](#) is available on the POAL website and intranet.

On induction all staff will be made aware of the operation of CCTV cameras including in container handling equipment.

7.4 Access

Images are only accessible by authorised personnel including licenced security staff, enforcement officers, performance coaches, supervisors, shift managers, health and safety managers or more senior managers for the purposes of investigation of

incidents or accidents, or for use in disciplinary procedures. Click here for the [process to request access to footage](#).

Those with authorised access to CCTV images must view and use the images only as intended. Images must not be shared with anyone who does not have authorised access, whether on monitors or mobile phones or any other media.

7.5 Written record

The Head of Security will keep a written record of all access to CCTV images by external parties.

7.6 Responsibility

Responsibility for the operation of the CCTV security system lies with POAL's Head of Security

Responsibility for the operation of the CHE CCTV system lies with the General Manager, Container Terminal Operations.

Responsibility for IT in relation to CCTV cameras lies with the IT Port Operations Team.

8 STORAGE, SECURITY AND DISPOSAL OF PERSONAL INFORMATION

POAL will ensure that all personal information, in either electronic form or hard copy, is protected against loss, against unauthorised access, use, modification or disclosure, or other misuse.

The [Information Security Charter](#) and [supporting cybersecurity standards](#) set out in detail the rules around the confidentiality, integrity and availability of all POAL information.

The Company's [Code of Ethics](#) requires all POAL people to maintain and protect the confidentiality of information entrusted to or generated by POAL.

POAL will not hold personal information for longer than is required for the purposes for which it may lawfully be used at which time it will be disposed of in a secure manner. For electronically held information refer to the [Information Security Charter](#). Hard copy information must be shredded.

8.1 Personnel Files

The People and Capability team maintains a virtual and physical Personnel File for every Employee. Where possible, information is stored in the virtual folder on POAL's servers. However, where hard copies have been generated, these are held in the individual's hardcopy Personnel File. All hard copy documents will be scanned so an electronic copy is also held.

The hard copy Personnel Files are stored in a locked shelving system. Only authorised staff have access to the keys to this system. Authorised staff are limited to selected members of the People and Capability team.

Electronic copies of Personnel Files are held in a secure folder on the Company's shared drive. Access is restricted to selected members of the People and Capability team, controlled by the System Administrator. These files are backed up regularly with all files held on the shared drive.

The exceptions to these standard storage arrangements are:

1. The hard copy Personnel Files of the Executive Team and People and Capability team are held in a locked cabinet within the Payroll Office. The only staff who have access to these files are the payroll team, the Deputy CEO & CFO and the Chief Executive Officer.

2. The electronic copies of the contracts relating to the Executive Team and the SM People Capability and Business Support are held in a secure folder on the shared drive. These are only accessible to the payroll team, SM People Capability and Business Support, Deputy CEO & CFO and the Chief Executive.
3. Performance management information relating to the Executive Team is held in a locked cabinet in the Chief Executive's Office.
4. Team leaders and managers may from time to time hold Personal or Performance Management Information in hard copy. All such information must be stored within a locked drawer or cabinet in their office when not in use and must never be left unattended when not in their locked drawer or cabinet.

Hard copy Employee Personal Information will only be kept until it is no longer required for the purposes for which it was collected. When an Employee ceases employment, their hard copy Personnel File will be held on site for one year.

After one year the Personnel File will be sent to a secure archiving facility for six years. The file will be destroyed at the end of the period.

Electronic copies of Personnel Files will be moved from the Current Employee folder to the Terminated Employee Folder within three weeks of the termination. Files will remain within the Terminated Employee folder for seven years. At the end of seven years, the folders will be archived and deleted from the network drive.

9 USE OF PERSONAL INFORMATION

POAL will not use personal information for any purpose other than the purpose for which it was collected unless authorised by the individual concerned.

10 ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

An individual is entitled to obtain from POAL confirmation of what personal information is held, to have access to the information and request the correction of the information.

Employees will need to complete a request form to [access](#) or [correct](#) information about themselves.

POAL will take all reasonable steps to ensure that the information it holds is accurate, up to date, complete and not misleading.

Employees should advise their manager and/or Payroll of any change of contact details. Payroll will regularly check that details are correct.

10.1 Personnel Files

All employees may ask to know what is contained within their personnel file and may request to view their own file. If they wish to view their own file they must apply in writing to the People Capability team. They may not request to view, or access, the file of any other person.

Direct managers of individuals may access that individual's personnel file if they have a specific work related reason to do so. If they wish to view one of their employees' files, the manager must direct their requests to the People Capability team stating their reason for needing to access the file. Managers may not request to view the file of someone who is not below them in their direct reporting line.

When a request has been made for an individual or their manager to view a personnel file, this must be arranged as soon as is practically possible. In normal circumstances this will be within three working days.

Files must be viewed within the presence of a member of a People and Capability Team. Hard copy files may not be taken away from the viewing room. Electronic

copies must be viewed on-line on a computer or device controlled by the People and Capability team member.

An employee may take copies of information contained within their own personnel file, provided that in doing so, it does not breach the privacy rights of others.

If a Manager requires a copy of any document within the personnel files, they may take a copy. They are required to store any copies within a locked drawer or cabinet in their office when not in use and must never leave documents containing Personal Information unattended when not in their locked drawer or cabinet.

11 DISCLOSURE OF PERSONAL INFORMATION

POAL will not disclose personal information to any third party without consent of the individual involved, except where allowed by the Act.

If a privacy breach occurs the [guidelines](#) provided by the Privacy Commissioner will be followed.

12 UNIQUE IDENTIFIERS

POAL will only assign unique identifiers to individuals where necessary, including but not limited to the following circumstances:

- An employee number for payroll purposes
- A user name for the purpose of signing on to the POAL server / computer system
- Security card for automatic access into secure sites.
- Unique identifiers assigned by POAL will not be the same as that assigned by any other agency (eg it will not be an individual's IRD number).
- POAL may require an individual to disclose a unique identifier where necessary (eg an individual's IRD number will be required to pay income tax or Kiwisaver payments).

13 CONTACTS

Email: PrivacyOfficer@poal.co.nz

POAL Privacy Officer

Governance & Risk Manager
Paul Milmine
Extension: 5248
Mobile: 021 770 254
milminep@poal.co.nz

Alternate Privacy Officer

Governance & Risk Advisor
Roslyn Johnstone
Extension: 5210
Mobile: 027 271 4050
johnros@poal.co.nz

Privacy Commissioner

PO Box 10-094
The Terrace
Wellington 6143
Telephone: 04-474 7590
Facsimile: 04-474 7595
email: enquiries@privacy.org.nz
Enquiries Line: 0800 803 909

Policy Owner: Governance & Risk Manager

Board Approval 16 November 2020

Review dates: Biennially

