

MEMORANDUM OF UNDERSTANDING
BETWEEN
AUCKLAND TRANSPORT
&
NZ POLICE

For shared use of
Closed Circuit Television (CCTV) Systems

27 June 2022

V4.0



Parties

1. This MOU is between:
 - a) Auckland Transport (“AT”); and
 - b) New Zealand Police (“NZ Police”);collectively referred to as “the Parties”.

Term

2. This interim MOU commences on the date it has been signed by the Parties and continues in effect until it is terminated in accordance with clause 43 or 44 (as applicable).

Purpose and Status of this MOU

3. The purpose of this MOU is to record the mutual understanding, expectations and arrangements between the Parties around:
 - a) the basis for sharing the use of CCTV systems between them;
 - b) what CCTV systems they will share the use of; and
 - c) how they will manage the shared use of the CCTV systems.
4. This MOU confirms the arrangements between the Parties based on a spirit of goodwill and cooperation. It is intended to constitute and create legally binding and enforceable obligations on the Parties.
5. This MOU is not an Approved Information Sharing Agreement under the Privacy Act and does not authorise any breach of the Information Privacy Principles in that Act.

Scope of this MOU

6. This MOU is intended to cover the Parties’ use of the shared CCTV systems and each Party’s access to CCTV footage captured by the shared CCTV systems to support each Party’s access to CCTV footage for their own individual lawful functions and purposes.
7. NZ Police and the NZ Transport Agency are parties to a separate memorandum of understanding allowing the NZ Police to use the NZ Transport Agency’s CCTV systems and CCTV footage in accordance with the arrangements set out in that memorandum. The Parties acknowledge AT’s entry into this MOU is premised on that memorandum of understanding between the NZ Police and the NZ Transport Agency remaining extant during the term of this MOU. This MOU does not cover the sharing of recorded CCTV footage captured by any CCTV camera that does



not form part of the shared CCTV system and held by any individual Party to any other Party (for example, as may be requested and/or required under the Local Government Official Information and Meetings Act 1987, Official Information Act 1982 or the Privacy Act 2020). Requests for sharing or disclosure of any CCTV footage held by any Party outside of the shared CCTV system are to follow the processes and protocol(s) separately agreed between the Parties.

Interpretation

8. In this MOU, unless the context otherwise requires, the following terms have the corresponding meanings set out below:

<i>access</i>	in relation to CCTV footage, may include viewing, controlling the capture of, or collecting the footage
<i>ATOC</i>	Auckland Transport Operations Centre (operated under joint partnership by AT and Waka Kotahi with collective responsibility for managing the upper North Island State Highway network and all other transport operations in the Auckland region, including all roads, public transport facilities, parking operations support and special events)
<i>authorised personnel</i>	employees and contractors of the Parties who have authorised access to the shared CCTV systems
<i>CCTV</i>	closed-circuit television
<i>CCTV camera</i>	closed-circuit television camera
<i>CCTV footage</i>	the moving and static imagery captured by a CCTV system, including live stream CCTV footage
<i>CCTV system</i>	closed-circuit television system, being any network of one or more closed-circuit television cameras connected to a recording system or monitor, by whatever digital means such system operates (e.g. digital or analogue) and includes the recording equipment, display equipment, transmission system, transmission media and interface control
<i>IPP</i>	means an Information Privacy Principle in the Privacy Act 2020



<i>live stream CCTV footage</i>	CCTV footage accessible as the imagery being captured is occurring in real time
<i>MOU</i>	means this Memorandum of Understanding
<i>Notifiable Privacy Breach</i>	means a privacy breach that it is reasonable to believe has caused serious harm to an affected individual or individuals or is likely to do so
<i>personal information</i>	means 'personal information' as defined in the Privacy Act 2020
<i>Primary User</i>	in relation to a CCTV system, means the agency that owns and maintains the CCTV system and uses it constantly for its own purposes, and <i>primary use</i> has a corresponding meaning
<i>Privacy Act</i>	means the Privacy Act 2020
<i>Privacy Breach</i>	means any unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, personal information, or any action that prevents a Party from accessing personal information on either a temporary or permanent basis
<i>Secondary User</i>	in relation to a CCTV system, means an agency that does not own the CCTV system but uses it for its own purposes on an as needs basis, and <i>secondary use</i> has a corresponding meaning
<i>shared CCTV systems</i>	the CCTV systems (or system components) agreed to be shared between the Parties as set out in Schedule 1

Background

9. AT is a council-controlled organisation (CCO), established under the Local Government (Auckland Council) Act 2009 with the primary function to contribute to an effective, efficient, and safe Auckland land transport system in the public interest. It manages the vast majority of Auckland's roads, public transport services (buses, ferries, trains and park-and-ride facilities) and public transport assets (bus stops, train stations and ferry terminals). AT also holds (under delegation from Auckland Council) Harbourmaster functions with respect to the Auckland harbour and is an airport authority with responsibility for managing the Great Barrier Island airfields at Claris and Okiwi.
10. NZ Police have the role and functions as set out in the Policing Act 2008 which are primarily focused around keeping the public safe from harm and preventing, investigating and enforcing against crime.



11. AT is a primary user of CCTV systems that capture and utilise CCTV footage across Auckland to support its individual lawful functions and activities.
12. NZ Police are a secondary user of certain CCTV systems that AT is a primary user of for the purposes of accessing live stream CCTV footage to support NZ Police's own lawful functions and activities.
13. The Parties collectively agree that the public interest benefits involved with sharing CCTV systems sufficiently supports a shared use approach.
14. The Parties wish to formalise their mutual understanding, expectations and arrangements for sharing the use of CCTV systems in the form of this MOU.
15. **Purposes for which the Parties use CCTV systems**
16. AT uses CCTV systems to support its statutory functions and functions that have been delegated to it under the Local Government (Auckland Council) Act 2009, in the following ways:
 - a) to support the safety and security of AT staff, AT customers and the general public using AT-controlled premises and the Auckland transport system;
 - b) to provide travel information;
 - c) to support the protection and security of public assets and facilities;
 - d) to support the prevention, detection, investigation, and enforcement prosecution of offences for which AT holds enforcement powers;
 - e) to support effective resolution of issues and complaints involving public services;
 - f) to support effective management and optimisation of the Auckland transport system through monitoring of traffic (including pedestrian traffic) on the road network and the operation of public transport services;
 - g) to monitor and manage events and operations such as construction projects and sporting events, that have an impact on the transport network to effectively manage the impacts and support smooth running of the network;
 - h) to support statistical analysis and research as part of AT's transport planning function; and
 - i) to support development of systems to improve the management, safety and optimisation of the Auckland transport system.
17. NZ Police use CCTV systems to support their statutory functions under the Policing Act 2008, in particular for:
 - a) maintaining public safety;
 - b) law enforcement;
 - c) crime prevention;
 - d) emergency management.



Rationale for the Parties to share the use of CCTV systems

18. The Parties consider that there is both operational and public interest support for sharing the use of CCTV systems between them in view of the significant cost and resource savings and efficiencies involved with a shared use approach.
19. The Parties also consider there is public interest in a shared use approach in terms of public safety benefits to be gained by NZ Police having access to the same CCTV systems as AT to support effective responsiveness of emergency services in the case of criminal and safety incidents on areas of Auckland's transport network under AT's control.
20. The Parties recognise that public interest support for a shared use approach is reliant on adequate measures being in place to ensure that each Party complies with its own legal obligations (particularly from a privacy law perspective) regarding the use of any shared CCTV systems, and the collection, use, storage and disclosure of any CCTV footage captured by any shared CCTV systems.

CCTV systems to be shared between the Parties

21. AT will share with NZ Police the use of the CCTV systems identified and as described in **Schedule 1**.
22. Secondary User access to CCTV systems by NZ Police will be in accordance with the Protocols and Procedures set out in **Schedule 2**.
23. Secondary User access for NZ Police will be granted on a case-by-case basis by AT and only where it is lawful to provide NZ Police with access to the CCTV system(s). Where NZ Police are provided access to a CCTV system, they will only be provided with access to CCTV footage to the extent that is necessary for NZ Police's lawful purpose in accessing the CCTV system.

Use of the shared CCTV systems

24. Each Party is individually responsible for meeting its own legal obligations in relation to its collection, use, storage and disclosure of any information obtained through use of the shared CCTV systems. This includes ensuring that the shared CCTV systems are only used to access CCTV footage where it has a legal basis for doing so, and only to the extent necessary to achieve the Party's lawful purpose in accessing the CCTV footage.
25. The Parties each acknowledge that where they access any personal information through their use of the shared CCTV systems, they act as an 'agency' as defined in the Privacy Act and are individually responsible for ensuring compliance with that Act with respect to that personal information (including in relation to the collection, use, storage and disclosure of the personal information).



26. As a Secondary user of the shared CCTV systems, NZ Police will only access and use the functionality of the shared CCTV systems as expressly permitted under **Schedule 1** and in accordance with the Protocols and Procedures in **Schedule 2**.
27. For the avoidance of doubt, facial recognition functionality (and any other artificial intelligence features) on any shared CCTV systems cannot be used by NZ Police as a Secondary User under this MOU, unless expressly permitted under **Schedule 1**.
28. Each Party individually accepts no responsibility for the actions of the other Party in using the shared CCTV systems.

Disclosure and subsequent use of CCTV footage captured by shared CCTV systems

29. Each Party acknowledges that it will be individually responsible for managing any personal information it collects via the shared CCTV systems, including ensuring that its disclosure of any personal information to the other Party or a third party is permitted under the Privacy Act, and that it only uses any CCTV footage disclosed to it as permitted by the Privacy Act.
30. The Parties consider that, to the extent that CCTV footage captured by shared CCTV systems may need to be disclosed between them, the following IPPs in the Privacy Act may be applicable to permit such disclosure and subsequent use:
 - a) IPP 11(1)(a) and IPP 10(1)(a) (directly related purpose); or
 - b) IPP 11(1)(e)(i) and IPP 10(1)(e)(i) (maintenance of the law); or
 - c) IPP 11(1)(e)(iv) and IPP 10(1)(e)(iv) (for the conduct of proceedings before any court of tribunal); or
 - d) IPP 11(1)(f)(i) or (ii) and IPP 10(1)(f)(i) or (ii) (to prevent or lessen a serious threat to public health or safety; or the life or health of an individual).
31. Clause 30 is only indicative of the IPPs that the Parties consider are most likely to be applicable and does not limit the application of and reliance by the Parties on any other IPP in any particular case.
32. Before disclosing or using personal information, each Party will consider and confirm that such disclosure or use is, in each case, permitted under the IPPs and other provisions of the Privacy Act.
33. If at any time a Party has doubt as to whether the use or disclosure of CCTV footage captured by any shared CCTV system is permitted under the Privacy Act, it will inform the other Party of its concern and cease any use or disclosure of the



CCTV footage until such time as it receives legal advice that the use or disclosure is permitted under the Privacy Act.

Access and Correction Requests

34. The Parties agree that individuals have a right to request access, and to seek correction of, their personal information held by either of the Parties. Each Party will comply with its obligations under the Privacy Act in relation to requests from individuals to access or correct their personal information.
35. As Primary User of the shared CCTV systems, AT has primary responsibility for managing requests for access to and/or correction of personal information collected by any of those systems. If a request for access to and/or correction is received by NZ Police, NZ Police will transfer the request to AT and inform the requester of the same, unless NZ Police has good cause to believe that the requestor does not want the request transferred to AT, in which case NZ Police will assume responsibility for managing the request.
36. The Parties will cooperate in response to requests for access to and correction of personal information. Each Party will provide all reasonable assistance to the Party managing the request, to enable that Party to meet its obligations under the Privacy Act.
37. Where a Party corrects any personal information or attaches a statement of correction, that Party must take reasonable steps to inform the other Party if it has disclosed such personal information to it.

Privacy Breaches

38. Each Party will comply with its obligations under the Privacy Act in relation to any Privacy Breach. Unless agreed otherwise in writing between the Parties, the Primary User of each CCTV system is responsible for notifying affected individuals and the Privacy Commissioner of any Notifiable Privacy Breach. Without limiting the foregoing, if a Secondary User learns of a Notifiable Privacy Breach and the Primary User fails to notify affected individuals and/or the Privacy Commissioner when it is required to do so, the Secondary User may give notice on behalf of the Primary User.
39. The Secondary User must notify the Primary User as soon as possible after becoming aware of any Privacy Breach.

Ownership of CCTV footage

40. CCTV footage that is recorded or downloaded to a Party's own systems is owned by that Party.
41. It may be possible for both Parties to download or record and therefore own the same CCTV footage.



Variations to this MOU

42. This MOU may only be varied with the agreement of both Parties, and any such variation shall be set out in writing and signed by the Parties.

Termination of this MOU

43. This MOU may be terminated by either Party giving one month's notice in writing to the other Party or as otherwise agreed in writing by the Parties.
44. If a Party breaches any term of this MOU in a non-trivial manner, this MOU may be terminated immediately in relation to the Party in breach, by the non-breaching Party giving notice in writing to the Party in breach.

Dispute Resolution

45. The Parties will negotiate in good faith to resolve any disputes arising out of, or in relation to, this MOU.
46. If resolution cannot be achieved at an operational level, the authorised representatives who have signed this MOU on behalf of each Party (or their equivalent authorised replacements) will work together to resolve the issue.
47. The terms of this MOU shall remain in effect pending any resolution of a dispute between the Parties in relation to this MOU.

External Communication

48. In the event that either Party receives a complaint or request for information in relation to the arrangements under this MOU, the receiving Party will consult with the other Party on the proposed response prior to responding to the complaint or request.

Review of this MOU

49. Either Party may request a review of this MOU at any time.
50. The Parties will collectively review this MOU in 12 months after it has been signed.


Costs

51. Each Party will bear its own costs in relation to any arrangements pursuant to this MOU.



Execution

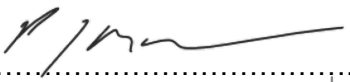
Signed for and on behalf of Auckland Transport

.....


Date: ...29/06/2022

Full Name:
John Strawbridge

Signed for and on behalf of New Zealand Police

.....


Date: ..25/07/2022

Full Name:
Inspector Peter McKennie
Acting Director: National Road Policing Centre

SCHEDULE 1

*To be agreed with the appropriate protocols in place

Component	System Description	Camera Groupings	Description	Primary User	Secondary User Access/Functionality			
					View	Control	Export	Notes/Comments
1. Vidsys	Auckland Transport's CCTV User Interface (UI) to access streaming AT CCTV.	Bus CCTV	CCTV at Bus Stations and facilities are PTZ and fixed	AT	NZ Police	NZ Police	NZ Police	
		Ferry CCTV	CCTV at AT operated wharves and facilities are PTZ and fixed	AT	NZ Police	NZ Police	NZ Police	
		Parking & Enforcement CCTV	CCTV at Off-Street car parks and Park and Rides are PTZ and fixed	AT	NZ Police	NZ Police	NZ Police	
		Train CCTV	CCTV at Train Stations and facilities are PTZ and fixed	AT	NZ Police	NZ Police	NZ Police	
		Road CCTV	CCTV at intersections and on road corridors are PTZ and fixed	AT	NZ Police	NZ Police	NZ Police	
		Special Vehicle Lane CCTV	CCTV for transit lane and bus lane enforcement	AT	NZ Police	NZ Police	NZ Police	Updated based on principle IPP 11a and IPP 11 e(i).
		Parks	CCTV covering footpaths in some central Auckland Parks are PTZ	AT	NZ Police	NZ Police	NZ Police	

SCHEDULE 1

Functionality definitions	
View	Ability to view live stream CCTV footage
Control	Ability to Pan/Tilt/Zoom (“PTZ”) CCTV camera(s)
Export	Ability to extract a copy of CCTV footage



PROTOCOLS AND PROCEDURES
FOR SECONDARY USER ACCESS TO SHARED CCTV SYSTEMS

PART A - GENERAL

Purpose

1. This Schedule contains a set of protocols and procedures to be followed by Secondary Users of the shared CCTV systems (as defined in the MOU) to ensure the effective operation, integrity and security of those systems is maintained.

Authorisation of Secondary User personnel to access shared CCTV systems

2. Any employees or contractors of a Secondary User must be authorised by the Owner Agency Relationship Manager before they may have access to the shared CCTV systems.
3. The Owner Agency Relationship Manager will facilitate the creation of a login
4. Once the Login is available the secondary user must complete the AT CCTV policy training module
5. Once the CCTV policy training has been successfully completed then the secondary user must request access to CCTV, this can be supported by the Owner Agency Relationship Manager

Operator skills and knowledge

6. All employees and contractors authorised as per clauses 2 to 5 above (“authorised personnel”) need to be suitably trained to operate the shared CCTV systems. The Owner Agency Relationship Manager will organise training of authorised personnel as and when required.

Confidentiality

7. Secondary Users will ensure that all information enabling its access to the shared CCTV systems (such as passwords, access codes) is kept confidential at all times and will ensure that all of its authorised personnel acknowledge and understand this obligation.



Security of information

8. Secondary Users will ensure that:
 - a) they have adequate measures in place to prevent unauthorised access, recording, exporting and disclosure of CCTV footage accessible through the shared CCTV systems; and
 - b) where information (including CCTV footage) accessed through the shared CCTV systems is kept or stored in any form that might be easily portable (e.g. printed material, laptop, portable digital assistant, DVD, CD, memory card or USB portable device) appropriate safeguards will be in place to guard against any unauthorised access, use or disclosure of the information. If the information is kept or stored on such a device for the purpose of transfer of source or comparison information, it will be permanently and securely disposed of once the transfer has been completed.

System faults or maintenance issues

9. Secondary Users are to report CCTV system faults or maintenance issues by logging an AT Assist incident via the 0800 AT ASSIST, who will arrange for the necessary repair or maintenance.

Requests for new CCTV cameras or changes to existing CCTV camera locations

10. The addition of new CCTV cameras to a shared CCTV system or changes to existing CCTV camera locations is at the discretion of the Primary User of the shared CCTV system.

Breaches of Protocols and Procedures

11. Operation of CCTV by Secondary users must be in accordance with AT's CCTV Policy, Guidelines, Procedures and Standards.
12. CCTV operations require high standards of integrity and honesty. The Secondary User will be responsible for any disciplinary action against any of its own authorised personnel who breach any of these Protocols and Procedures.



Termination of Authorised User access to shared CCTV systems

- 13. AT will terminate the access of an Authorised User when the NZ Police confirms that the Authorised User no longer requires access as part of his/her role with the NZ Police or ceases employment/contract with the NZ Police.
- 14. AT may otherwise, in its sole discretion, terminate the access of any Authorised User to the shared CCTV systems at any time (including in the case of any actual or suspected breach of these Protocols and Procedures).

Relationship Management and Oversight

- 15. To facilitate and support the relationship between the Parties in this MOU, and to provide operational oversight over the sharing of access to CCTV footage, each Party will nominate a Relationship Manager.
- 16. The Relationship Managers primary role is to provide oversight to the operation of this MOU as follows:
 - a. be the first point of contact
 - b. manage access to the shared CCTV system and provide assistance if required
 - c. arrange CCTV system training
- 17. The Relationship Manager(s) for each Party are identified in the below table

Party	Relationship Manager Name	Title	Contact Details
Auckland Transport			
NZ Police			

**PART B****Special protocols and procedures where NZ Police is the Secondary User****Scenario 1: Operator Assistance in the case of a real time serious incident or threat:**

1. Police to go to their DCC and city cameras first prior to contacting the TOC (for non-transport related incidents/events)
2. If DCC or City cameras are unable to assist then Police to phone/contact the TOC Operations Room lead, TOC Shift Lead, Team Leader or Senior Operator and provide:
 - a. Description of the assistance required
 - b. Which Camera(s)
 - c. Duration required
 - d. Provide contact details at Police
 - e. TOC Operator assists Police with the incident
3. Once the incident is completed then Police are to confirm this back to the TOC Operations Room lead, TOC Shift Lead, Team Leader or Senior Operator

Scenario 2: Taking control of Camera(s)

In this scenario TOC and Police want to control the same camera at the same time.

1. Police to phone/contact the TOC Shift Lead or Senior Operator
2. Police to describe the incident /event that requires control of the camera(s)
3. If the TOC Operations Room lead, TOC Shift Lead, Team Leader or Senior Operator agrees that Police can take control of camera(s):
 - a. Then Police to provide:
 - i. Which camera(s)
 - ii. Duration required
 - iii. Provide contact details at Police
 - iv. Police take control of the camera(s)
 - b. Once the incident is completed then Police are to confirm this back to TOC Operations Room lead, TOC Shift Lead, Team Leader or Senior Operator
4. If the TOC Shift lead believes TOC priority is higher than Police need, then TOC escalation process kicks off as per the ATOC Standard Operating Procedure.



Scenario 3: The Blocking of Camera(s)

For any camera that Police want to block :

1. Phone/contact the TOC Operations Room lead, TOC Shift Lead, Team Leader or Senior Operator
2. Police describe the incident /event that requires a block
3. If the TOC Operations Room lead, TOC Shift Lead, Team Leader or Senior Operator agrees that Police can take control of camera(s):
 - a. Then Police to provide:
 - i. Which Camera(s)
 - ii. Duration required
 - iii. Provide contact details at Police
 - iv. Blocking feature is applied to camera(s)
 - b. Once the incident is completed then Police to confirm this back to the TOC Shift Lead
 - c. Block is removed from the camera(s)
4. If the TOC Shift lead believes TOC priority is higher than Police need, then TOC escalation process kicks off as per the ATOC Standard Operating Procedure.

Monthly Meeting between TOC and Police

To facilitate and support the ongoing relationship between Police and the TOC the introduction of a monthly meeting will be established. At this meeting Police and TOC will discuss/review incidents in the past month and agree the lessons learnt. This will enable the teams to continue to improve the process going forward.