Closed Circuit Television Policy (CCTV)

1. What is this policy about?

Auckland Transport (AT) uses **Closed Circuit Television (CCTV)** systems to support its transport functions and activities by enhancing public safety, improving operational efficiency, and meeting legal obligations while safeguarding individual privacy. **CCTV systems** are installed, operated, and managed in line with clear governance standards that ensure footage and data are collected, accessed, and used responsibly.

CCTV is used consistently across Auckland's transport network through clearly defined roles and procedures, helping ensure footage is handled appropriately and systems are aligned across different environments and operators.

This Closed Circuit Television (CCTV) policy sets out how AT will install, operate, and manage CCTV systems, and how it will collect, use and manage **CCTV footage** and **CCTV data** including **Automatic Number Plate Recognition (ANPR)**.

2. Who does it apply to?

This policy applies to all AT employees and AT representatives (such as contractors, consultants, agency temps, external staff on secondment). Transport service operators who collect, use, or manage CCTV under the terms of contracts with AT. Auckland Council and Council-Controlled Organisations where CCTV systems are operated on or migrated to AT's platform under shared governance arrangements, e.g. Group Shared Services.

Where this policy uses pronouns like "you", "your", "we", or "us", it is referring to anyone listed above, who this policy applies to.

When we talk about CCTV we are referring to all CCTV systems and equipment used, owned, operated or managed by AT, including CCTV on trains, roads, vehicles, carparks, airfields, **drones (Unmanned Aerial Vehicles),** in buildings, rail stabling and maintenance yards, rail level crossings, body-worn cameras on AT staff and ANPR information.

It also includes the following CCTV systems, which are not managed by AT:

- CCTV systems operated on board ferries or buses that are owned and managed by the operator.

- CCTV systems operated on State Highways and other transport assets, which are managed by NZ Transport Agency/Waka Kotahi (NZTA), and operated through the Auckland Transport Operations Centre (ATOC), where AT has operational involvement or access.

- CCTV systems operated on some ferry wharves, which are not managed or operated by AT.

- CCTV systems which are part of the Safer Cities vGrid network and access AT cameras.

- Local Boards' or other community-based CCTV systems to which AT has access.

This policy does not apply to the NZTA and the use of CCTV systems it owns. Where AT staff or contractors are granted access to NZTA owned CCTV systems (e.g., via ATOC), such access must be in accordance with NZTA's access and usage policies.

3. How we use CCTV

AT uses CCTV systems to support its powers, functions, and duties under the Local Government (Auckland Council) Act 2009 or otherwise delegated to it, in the following ways:

- to support the safety and security of AT staff, AT customers and the public using **AT premises** and the **Auckland transport system** and associated transport network

- to provide travel information

- to support the protection and security of public assets and facilities

- to support inspections and remote working

- to support the prevention, detection, investigation, and enforcement of offences for which AT holds enforcement powers

- to support effective resolution of issues and complaints involving public services

- to support effective management and optimisation of the Auckland transport system through monitoring of traffic (including pedestrian traffic) on the transport network and the operation of public transport services

- 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 the smooth running of the network

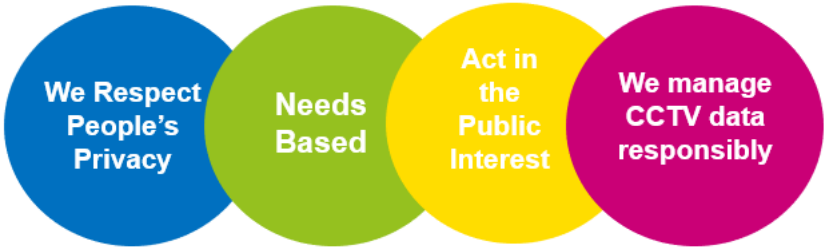
- to support statistical analysis and research to support AT's transport planning function

- to support the development of systems to improve the management, safety and

optimisation of the Auckland transport system.

4. Principles that guide us

At AT, the responsible use of CCTV is guided by clear principles that protect both public safety and individual privacy. These expectations apply to all personnel operating CCTV systems on behalf of AT. Staff using CCTV systems must adhere to the Code of Conduct Policy and perform their duties in accordance with the AT CCTV Standards and Procedures.



If you have questions about CCTV systems, footage, or data management, please contact the CCTV Product Owner. They can provide guidance on applying the policy correctly and support you in ensuring CCTV data is handled securely and responsibly.

4.1. We respect people's privacy

AT is committed to safeguarding individual privacy by collecting and using CCTV footage only for legitimate operational, safety, and security purposes. Staff won't use CCTV to monitor private property unless there's a valid, approved reason for it (see How we use CCTV).

Any personal information collected or shared via its CCTV systems is handled in line with the Privacy Act 2020 and AT's Privacy Policy when dealing with personal data.

4.2. Needs based

CCTV systems will only be installed and used when there's a clear need based on one or more approved purposes set out in this policy. Each setup must be signed off by the CCTV Operational Governance group.

If changes are needed like adjusting camera types or installation locations those updates must be approved by the CCTV Product Owner and reported back to the Governance Group.

4.3. Act in the public interest

AT recognises the importance of balancing operational effectiveness with the privacy rights of the public. The following principles outline AT's approach to ensuring that its use of CCTV systems is transparent, responsible, and respectful of lawful public activity:

- AT does not identify individuals in CCTV data or footage unless it is needed for lawful

purposes.

- Appropriate notification will be in place whenever practicable to inform the public that CCTV systems are in operation.

- The CCTV policy and related information is available on the AT website. CCTV related enquiries and complaints can be made via CCTV Management at Auckland Transport and Official information requests.

- AT managed public streaming (e.g., displays at stations or online feeds showing platform activity) is permitted where it serves a legitimate safety or operational purpose and is subject to AT's privacy and governance controls.

- All other live streaming access, including by contractors, vendors, or external agencies, must be restricted to authorised personnel only. Any exceptions must be formally approved by the CCTV Strategic Governance Group.

4.4. We manage CCTV data responsibly

AT manages CCTV data responsibly to protect people's privacy and ensure the data is used appropriately. This includes clear rules around who is responsible for and manages the data, how long it's kept, who can access it, and how it can be shared. All CCTV data is handled in line with AT's policies, legal requirements, and approved procedures to make sure it's secure and only used for the right reasons.

CCTV Recordings

- CCTV data collected or processed through CCTV systems owned or managed by AT is the property of AT

- CCTV data collected on buses and ferries is owned by the respective operator (unless otherwise provided under contract with AT)

- The monitoring, retention, storage and destruction of CCTV data and images will be closely regulated using CCTV standards, procedures and guidelines agreed by the CCTV Strategic Governance Group

- CCTV data collected and retained must be accurate, relevant and must not exceed that which is necessary to fulfil the purpose for which it is collected.

- Access to recorded images must be restricted to authorised persons only or as otherwise required by law.

Retention

CCTV footage and CCTV data will be retained in accordance with AT's Information and Records Management Policy and the CCTV Standards. CCTV data will only be kept for as long as is necessary to fulfil the purpose(s) for its collection.

- If CCTV data becomes a **Protected Record,** it is kept indefinitely (unless otherwise instructed by the Chief Archivist).

- Where the purpose of the collection requires CCTV footage or CCTV data to be retained for a longer period than specified in the CCTV Standard or where there is a legal requirement to do so, AT will remove personal information contained within such footage or data unless it is required for the purpose of the retention of the footage.

Release of CCTV information

Release of CCTV footage and/or CCTV data to organisations and individuals will be managed in accordance with CCTV procedures, and legislation including the Privacy Policy, and Local Government Official Information and Meetings Act (LGOIMA) requirements.

- Public seeking release of data may make a request via AT's CRM. Requests will be forwarded to the LGOIMA Team. When authorising the release of CCTV information, the AT Privacy Policy and AT Delegations Register (Schedule 21) as outlined in CCTV Procedures, must be followed.

- AT staff are required to submit a request via ServiceNow, depending on where the request originated it is passed to the appropriate team.

- Release of CCTV data that is **structured data**, as defined in the AT Data Policy, must be in accordance with that policy.

- CCTV footage will not be released if this is not permitted by law.

- Any ongoing arrangements for access to CCTV systems or release of CCTV footage/data to third parties must be formalised in writing, approved by the CCTV Operational Governance Group, and signed off in accordance with AT's Delegations Register.

Security of CCTV footage

Appropriate security measures must be taken to protect against unauthorised access to, alteration, disclosure, loss or destruction of CCTV footage and/or CCTV data.

Security measures will include physical, technological and administrative means. These include ensuring only authorised persons have access to the CCTV software, restricting permissions to those needed to perform their duties, and annual reviews of access rights.

5. Automatic Number Plate Recognition (ANPR)

ANPR is the recognition of number plates in CCTV footage. It records the number plate along with the date, time and location of the vehicle.

5.1. Purpose of ANPR Use

AT uses ANPR technology to support a range of operational and enforcement functions, including but not limited to:

- Monitoring and managing access to restricted areas such as bus lanes and carparks.
- Supporting traffic flow analysis, transport research and planning.
- Enabling enforcement of parking and traffic regulations.
- Identifying and responding to stolen vehicles and other criminal offending in collaboration with NZ Police.

5.2. Collection and Storage of ANPR Data

ANPR data is collected through fixed and mobile cameras located across the AT, including carparks, arterial roads, and enforcement zones. The data collected includes vehicle number plates, timestamps, and location metadata.

- Data collected for enforcement purposes (e.g., bus lane infringements) is retained for up to 7 years as legal evidence.
- Non-evidential footage is typically retained for 7 days before being overwritten.
- ANPR metadata will be encrypted and stored for 3 years or until no longer required.

5.3. Use and Disclosure

ANPR data is used for the purposes for which it was collected, in accordance with AT's Privacy Policy and the Privacy Act 2020. This includes:

- Enforcement actions by AT or delegated authorities.
- Sharing with NZ Police and other regulatory authorities under formal agreements for stolen vehicle identification and public safety.
- Sharing with CCO's for the control, management and enforcement of related carparks.
- Research and planning purposes, where data is anonymised and aggregated.

5.4. Public Notification and Signage

In accordance with the Privacy Act, where possible, AT ensures that individuals are made aware of ANPR data collection through:

- Signage at carparks and enforcement locations.
- References in AT's publicly available CCTV and Privacy Policies.

5.5. Access and Security

Access to ANPR data is restricted to authorised personnel only. All access is logged and subject to audit. Data is stored securely within AT's infrastructure and protected from unauthorised access.

5.6. Governance and Oversight

The use of ANPR is governed by AT's CCTV Strategic Governance Group.

6. Audit and Assurance

To ensure that AT's use of CCTV and the associated data is consistent with this policy and associated procedures, standards and guidelines, AT will regularly monitor and review how CCTV is used and managed across the business. The CCTV Product Owner has oversight and responsibility for ensuring the reviews occur regularly and may be supported by other assurance teams at AT, such as Internal Audit or Compliance.

7. Key Terms

Term	Definition
AT premises	This includes AT-controlled bus, ferry, and train stations, off-street carparks controlled or managed by AT, AT offices, and other premises that AT owns or controls or uses (under delegation or otherwise). AT also manages two Great Barrier airfields on behalf of the Auckland Council.
Auckland Transport system	As defined in section 37 of the Local Government (Auckland Council) Act 2009 – means – (i) the roads (as defined in section 315 of the Local Government Act 1974) within Auckland; and

Term	Definition
	(ii) the public transport services (as defined in section 5(1) of the Land Transport Management Act 2003) within Auckland; and (iii) the public transport infrastructure owned by the Council; and (iv) the public transport infrastructure owned by or under the control of Auckland Transport; but does not include – (i) State highways; (ii) railways under the control of New Zealand Railways Corporation; (iii) off-street parking facilities under the control of the Council; (iv) airfields (other than the Great Barrier).
Automated Number Plate Recognition (ANPR)	Technology used to automatically read motor vehicle number plates using optical character recognition.
CCTV data	CCTV data is the data collected by a CCTV system.
CCTV footage	The moving and static imagery is captured by a CCTV system.
CCTV systems	The CCTV system includes the recording equipment, including drones, display equipment, transmission system, transmission media and interface control.
Closed-Circuit Television (CCTV)	CCTV is a camera surveillance system that captures images that may include individuals or information relating to individuals.
Drones (Unmanned Aerial Vehicles)	A powered aerial vehicle that does not carry a human operator, capable of autonomous or remote-controlled flight, and may carry cameras or other payloads for surveillance, monitoring, or operational purposes.
Event	This includes planned and unplanned events.

Term	Definition
Protected Record	A Protected Record as defined in the Public Records Act 2005.
Structured Data	Data formatted into a well-defined model, usually stored in a structured database.

8. Roles and Responsibilities

Role	Responsibility
All Employees and AT Representatives	• Adherence and compliance with this policy and related procedures.
Chief Executive	• Approves the CCTV policy. • Promotes the principles of the CCTV policy.
Chief Technology Officer (Policy Owner)	• Has overarching responsibilities for the CCTV policy. • Oversees the management of CCTV.
CCTV Operational Governance Group	• Advise on CCTV operational matters. • Review/ approve/ decline requests for CCTV based on agreed standards and in line with CCTV policy and guidelines. • Advise on opportunities to improve operational and customer experience.
CCTV Product Owner (Policy Contact)	• Responsible for managing overall policy, and procedures and alignment with privacy, legal, and operational standards. • Overall oversight of CCTV system access and data release. • Sponsor information sharing agreements for CCTV. • Approves and reviews camera changes.
CCTV Strategic Governance Group	• Advise on significant strategic AT camera changes, issues, risks, and organisational priorities. • Review CCTV policy, CCTV Information Sharing Agreements, signage and privacy changes.

Role	Responsibility
Privacy Officer	• Providing support and direction about how AT uses CCTV in line with privacy policy and legislation. • Ensure AT complies with the information privacy principles in the Privacy Act 2020. • Responds to privacy requests. • Receives Privacy complaints.

Operational responsibilities of these roles can be found in the CCTV Roles and Responsibilities document.

9. Supporting Information

Legislative compliance	This Policy supports AT's compliance with the following legislation: • Local Government Official Information and Meetings Act 1987 • Privacy Act 2020 • Public Records Act 2005 • Local Government (Auckland Council) Act 2009
Supporting documents	These are listed in the Policy Hub on the AT intranet. • CCTV Standards • CCTV Procedures • CCTV Guidelines • CCTV Roles and Responsibilities • Information and Records Management Policy • Information Security Policy • Identity and Access Management Security Standard • Acceptable Use Policy

	• Privacy Policy • Code of Conduct Policy • Body-worn Cameras Operational Business Process • AT Data Policy
Related documents	• Civil Defence National Emergencies (Information Sharing) Code 2013 • Pointers for security cameras and drones (UAV), Office of the Privacy Commissioner guidelines • Privacy and CCTV, Office of the Privacy Commissioner guidelines

10. Non-Compliance

Any breach of this policy may result in disciplinary action, as outlined in AT's Code of Conduct Policy, or lead to a contractor's agreement being terminated. CCTV footage may also be used as part of any disciplinary process, in line with that policy.

11. Approval & Review

Policy Owner: Chief Technology Officer **Policy Contact:** CCTV Product Owner

Approved by: Dean Kimpton

Chief Executive

Approval date: 20/11/2025

Effective date: 15/12/2025 Next review date: 15/12/2028

AT reserves the right to review, amend or add to this policy at any time upon reasonable notice to employees and representatives.