Office of the
State Archivist

Records from surveillance technologies

IMPLEMENTATION TOOL

INTRODUCTION

It is a common misconception that you only need to keep surveillance footage for 30 days. This is correct for closed-circuit television (CCTV) property surveillance footage. But different retention periods apply when surveillance is used for different purposes. Like all other records, retention periods range from short-term to permanent.

This tool provides examples of types of technologies, their uses and retention periods.

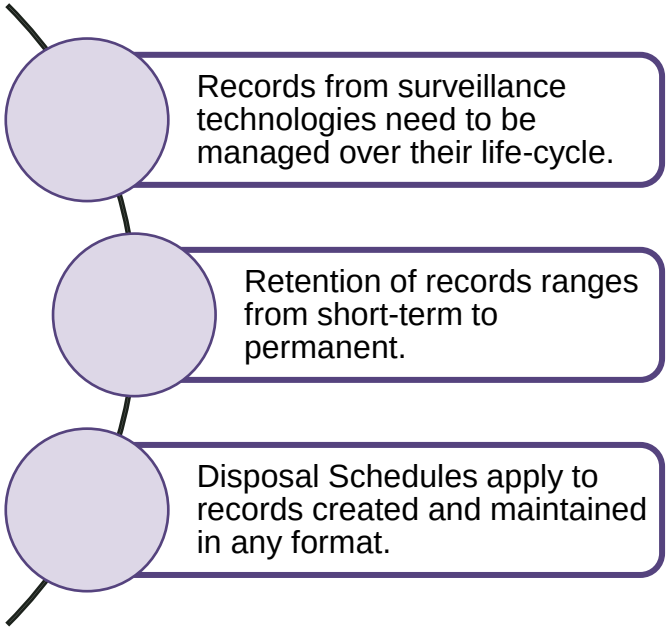
It does not cover records of mass surveillance, or police surveillance operations.

GENERAL ADVICE

State and territory laws restrict surveillance in certain circumstances. Ethics, governance, privacy, and the law have yet to catch up with surveillance. We cannot provide advice on these issues, but we do recommend you:

- research technologies and their wider implications
- seek guidance on ethics, governance, human rights, and privacy from relevant authorities
- seek legal advice.

KEY MESSAGES



Tasmanian Government

Contents

WHAT ARE SURVEILLANCE TECHNOLOGIES?

Surveillance is the monitoring and analysis of data to collect information about places, persons, or things.

Surveillance technologies may be:

- listening devices that can listen or record conversations
- optical devices that observe or visually record activities
- data devices that monitor or record the input and output of information to and from a computer
- tracking devices that determine the geographical location of a person or thing
- combinations of one or more of these devices.

Examples of old surveillance technologies include:

- audiovisual recordings
- CCTV
- fixed road safety cameras.

Recent technologies include:

- ankle bracelets
- drones
- workplace surveillance.

New surveillance technologies can collect, intercept, keep, analyse, process, and share information. They can be combined with artificial intelligence (AI) or automated decision-making (ADM) technologies.

RECORDS MANAGEMENT ADVICE

Managing your records

Our *Information and records management standard* describes requirements for managing records.

Like all other records, you need to manage records from surveillance technologies over their life-cycle. This means you need to keep them accessible for as long as needed.

Policies and procedures

You may need to update or create organisational policies and procedures to cover surveillance and recordkeeping including:

- primary, original, and working versions
- legal requirements
- audit trails
- metadata management
- file formats
- storage
- access and third-party handling
- security and privacy settings
- outsourcing
- child-related records
- retention and disposal.

Child-related records

We have two current Disposal Freezes on child-related records. This means you cannot destroy records covered by either freeze. (*Example 3*.)

You may need new policies and procedures to deal with surveillance records and children.

Records as evidence

Australia and New Zealand guidelines for digital imaging processes is for forensic and law enforcement organisations using digital images as evidence. Records staff may also find it helpful.

It gives details on:

- preparation
- capture
- use (including image processing and compression)
- retention and disposal
- primary, original, and working versions.

Primary, original, and working versions

Primary versions are removed from devices in their native format without compression or change.

Original versions (master or preservation copies) are the state record. These are exact copies of the primary version. Store original versions without compression. Compression can reduce quality and make records unusable.

Working versions are copies of the primary or original version. Working versions allow you to enhance, alter, filter and crop. You can also use these as access copies.

Sustainable file formats

Sustainable digital file formats for creating and using records has a list of recommended file formats, including audio and video.

Disposal Schedules

Disposal Schedules describe government functions and activities. They tell you how long to keep records before:

- destroying them or
- transferring them to the Tasmanian Archives.

Retention of records from surveillance technologies ranges from short-term to permanent.

Retention periods in disposal schedules reflect:

- business needs
- legal and regulatory requirements
- community and societal expectations.

Disposal Schedules apply to records created and maintained in any format. They rarely mention technologies or formats of records. Identify the function or activity the technology supports to find its retention. *(Example 10.)*

Sometimes Disposal Schedules *do* mention specific technologies. Use common sense when applying the retention to another technology. *(Example 1*.)

Introducing surveillance technologies often creates related records, for example:

- policy
- legal advice
- privacy assessments
- infringements
- decommissioning.

You also need to manage and keep these records, and they may have different retention periods. *(Examples 11, 13 and 14.)*

You may need to look in several Disposal Schedules to find coverage of records.

How long to keep records

Retention periods in Disposal Schedules are minimum periods. If you have a business need for records, you can keep them longer but take a risk-based approach. Consider:

- the personal information the records contain
- the risk from a data breach
- management and storage costs.

Records retention ranges from short-term to permanent. You can use *Disposal Schedule for short term value records* (DA2158) to destroy some records. *(Example 8*.)

If you use records for another purpose, this may change the retention period. *(Examples 4 and 7*.)

If you use records for more than one purpose, and you could apply many record classes, keep them for the longest retention period.

Unscheduled records and Destruction Authorities

Unscheduled records are records not covered by any disposal schedule. Unscheduled records include all pre-1960 records.

To dispose of unscheduled records, ask us for a Destruction Authority. This is a one-off authorisation from the State Archivist that allows you to destroy specific records.

When you cannot destroy records

Sometimes you cannot destroy records even if the retention period has passed. This includes records covered by a Disposal Freeze and records needed for legal matters, including investigations and inquiries.

The introduction in our Disposal Schedules list all the exclusions.

Planning for the future

Use of surveillance technologies is growing. Technologies may be introduced without an understanding of records implications. We have already been asked whether records can be destroyed early because of storage costs.

Getting involved at the planning stages of introducing new technologies reduces risk. It means you can offer your expertise on potential issues before they come a problem. For example, you can confirm which government functions the technology supports. This means you can explain record retentions and estimate storage costs.

AI and other new technologies can perform tasks human cannot. This may help manage records through:

- auto-classification and labelling
- advanced search and retrieval
- mass-analysis of large amounts of data
- predictive analytics
- identification of sensitive records
- flagging records past their retention period.

SURVEILLANCE TECHNOLOGIES AND RECORDS RETENTION

This section includes examples of surveillance technologies in government, their uses and retention periods.

Check the relevant Disposal Schedule for full details: text and retention periods have been summarised.

Ankle bracelets (electronic monitoring bracelets)

Ankle bracelets are a wearable technology. They use radio frequency beacons, GPS, Wi-Fi or 4G to record the real-time location of the device and send coordinates to a control centre.

They can have exclusion zones that trigger an alert if the wearer enters this zone.

Ankle bracelets track locations of:

- people on bail or parole
- family and domestic violence perpetrators
- sex offenders
- terrorists.

Artificial intelligence (AI)

The development of computer systems or machines that perform tasks requiring human intelligence. Tasks include:

- data analysis
- natural language processing
- problem solving
- decision making.

Some of the surveillance technologies in this document include AI. For example, smart city technologies, speed cameras, voice assistants.

Some AI applications may not be recognised as AI. The AI may:

- be hidden or unknown (for example, traffic management, recruitment vetting)
- have been added to an existing technology (speed cameras, vacuums) or
- have become so common it is now ‘just another technology’ (chatbots, spam filters).

We will produce separate advice on recordkeeping and AI.

Audiovisual technologies

Audiovisual technologies include sounds and images. Examples include:

- films
- videos
- recorded lectures
- slideshows
- online streaming.

Government use of audio, visual and audiovisual technologies includes:

- audio recordings (for example emergency ‘000’ calls)
- closed-circuit TV recordings (CCTV)
- footage from body cameras, dashcams or drones
- online streaming of conferences, live events, or webinars
- recordings of meetings (for example Council meetings).

Example 1: Audio recordings (council meetings)

Audio recordings of meetings are made to help prepare minutes. You can destroy the recordings once the minutes are confirmed at the next meeting.

Note: This retention period will increase when we review *Disposal Schedule for functional records of local government* (DA2200).

The master set of minutes, agendas, terms of reference and related papers of Council and its Committees are permanent records.

While the Disposal Schedule specifically refers to audio recordings, you can also use this retention for video recordings.

Disposal Schedule for functional records of local government (DA2200), 13.04.03, 13.04.01.

Biometric data

Biometric data identifies and authenticates people through unique characteristics.

Biometric data can be:

- physical (for example DNA, fingerprints) or
- behavioural (for example gait, typing recognition).

The personal and often permanent nature of the data raises privacy concerns, especially when used for surveillance purposes.

Government use includes:

- access to services through facial, voice or fingerprint authentication
- automated passport control uses facial recognition and ePassports.

Example 2: Biometric data (Corrective Services)

Tasmanian prisons collect biometric data from visitors (fingerprints and iris scans). You can destroy visitor data when reference ceases.

Prisons also collect data from inmates. Inmates may apply to have their data destroyed, including photographs, fingerprints, and palm prints. You can destroy inmate data a year after their custodial sentence has ended or a year after their release.

Disposal Schedule for functional records of the Tasmanian Corrective Service (DA2330), 04.22.05, 01.03.08.

Body worn cameras (BWC or bodycams)

Body worn cameras record audio and video footage. They are worn on the torso or built into a helmet. These wearable technologies capture evidence of incidents and are a crime deterrent.

Bodycams are used by:

- police officers
- driving assessors to record driver test assessments
- park rangers and parking inspectors for compliance and enforcement activities
- school crossing guards to identify dangerous drivers.

Example 3: Body worn cameras (AYDC)

Youth workers at Ashley Youth Detention Centre (AYDC) use body worn cameras:

- for the safety of young people and staff
- for security
- to capture an accurate record of incidents.

Context: You cannot destroy records if:

- a Disposal Freeze is in place
- an investigation or inquiry is in progress, or
- they may be needed as evidence in a current or future legal matter.

The State Archivist has issued two Disposal Freezes on child-related records. Even when we lift the Disposal Freezes, and legal action and the redress schemes have ended, these are long-term records. (The forthcoming *Disposal Schedule for the care and protection of children and young people* (DA2585) will cover youth detention records.)

You need to keep records of child abuse allegations and incidents for 125 years after the date of birth of the child.

Disposal Schedule for records relating to child abuse (DA2520), 2.1.

Example 4: Body worn cameras (local councils)

Parking inspectors wear body worn cameras when issuing parking infringements. When legal action results, you can destroy footage seven years after the action is complete. If no legal action results, you can destroy footage three years after action is complete.

Context: These records support the compliance of laws and enforcement (infringements) function of government. When used for other purposes, the retention period may change.

For example, footage that captured an assault on a parking officer that led to their death. You would keep the relevant footage of the assault as part of the work health and safety investigation report as a permanent record.

Disposal Schedule for functional records of local government (DA2200), 19.05.01, 19.05.02, 21.13.01.

Closed-circuit television (CCTV)

CCTV systems use cameras to record video (and sometimes audio). Footage is sent to a control centre. CCTV is a crime deterrent in public places and used by police to solve crimes.

Other uses include:

- safety on public transport – drivers can check passengers are clear of doors before closing them
- monitoring visitors, and to deter bullying and vandalism in schools
- detecting traffic congestion and accidents
- reading licence plates in restricted zones to ensure compliance
- workplace surveillance.

Example 5: CCTV (security, property management)

You can destroy footage not needed for criminal investigations when reference ceases. This is typically one month. Footage required for criminal investigations can be destroyed after the end of the investigation and any legal proceedings.

Note: Retention of property surveillance footage is inconsistent in our schedules. We will resolve this when we update *Disposal Schedule for common administrative functions* (DA2157) and *Disposal Schedule for functional records of local government* (DA2200).

Example 6: CCTV (Tasmania Police station watch houses)

CCTV footage of incidents in watch house charge rooms that require police investigation or action. You can destroy this footage six months after you have copied images for the investigation file.

Disposal Schedule for functional records of the Department of Police and Emergency Management (DA2351), 02.25.06.

Dashboard cameras (dashcams)

Dashboard cameras capture sound, video, and GPS to keep a record of incidents or accidents. Some start recording automatically when the car starts.

Typically used in government to provide evidence for insurance:

- garbage trucks fitted with dashcams can provide evidence of damaged fences, property, or parked cars.

Example 7: Dashboard cameras (local councils)

Footage of accidents or incidents is included in investigation reports. You can destroy footage seven years after action is complete.

Context: Installation of dashcams supports council fleet management and insurance.

If footage is used for other purposes, the retention period may change. For example:

- Footage of an incident resulting in a workers compensation claim. In this case, the retention is long term. You can destroy the footage when the employee reaches 75 years old or seven years after action is complete, whichever is later.
- Footage of a car accident and a member of the public. If death results, the retention becomes permanent.

Disposal Schedule for functional records of local government (DA2200), 22.06.01, 27.01.01, 27.01.02.

Database surveillance

Databases containing personal data collected from a wide range of sources.

Public records may include marriage, property, car registration and criminal history. Private records may include work history, financial, DNA and social media.

Individuals, governments, and organisations can now buy information instead of seeking it through legal channels.

Immigration and law enforcement are typical government users.

Drones (unmanned aerial vehicles or UAVs)

Drones are small aircraft that work autonomously or by remote control. They can take photographs or video and deliver packages.

Government uses include:

- assessing fire risk and tracking the path of bushfires
- detection of unfenced swimming pools or illegal buildings
- inspections of bridges, dam walls, electricity poles and rail tracks
- mapping
- monitoring rare or endangered plants and animals in national parks
- search and rescue operations using thermal imaging cameras
- water quality monitoring
- weed management programs.

Example 8: Drones (TasRail inspections)

Drones inspect rail infrastructure, including bridges and culverts for defects. You can destroy footage ten years after action is complete.

Disposal Schedule for functional records of TasRail (DA2460), 7.7.1.

Context: Drones can take photographs and video footage. You only need to keep relevant records – this may be only minutes from hours of footage. You can use *Disposal Schedule for short term value records* (DA2158), 01.01.06 to destroy irrelevant photos or footage.

However, sometimes all footage is relevant. For example, records of major or significant fire incidents are permanent.

Disposal Schedule for functional records of Parks & Cultural Heritage (Department of Primary Industries, Parks, Water & Environment) (DA2489), 9.2.2.

Example 9: Drones (local council compliance)

Drones take photos or videos to ensure compliance with standards. For example, to detect illegal swimming pools. You can destroy footage seven years after action is complete.

Disposal Schedule for functional records of local government (DA2200), 18.03.01

Global Positioning System (GPS)

GPS is a network of satellites and receiving devices that give location in latitude, longitude and altitude and an accurate time. GPS can track:

- buses for real-time public transport arrival and departure information
- employees for safety in remote locations or on large building sites.

Location-based apps

Apps that provide users with information or services based on their geographic location. Map, weather and fitness apps are common examples.

Government uses include:

- emergency apps that send alerts for nearby fires and floods
- tourism apps allow users to build and save itineraries and receive live updates based on their location.

Remote invigilation (online proctoring software)

Used when students take online exams to reduce the likelihood of cheating. Software and artificial intelligence monitors and records activity on the student's computer, microphone, and webcam. It also identifies suspicious behaviour for human review.

Example 10: Remote invigilation (University of Tasmania)

Administrative arrangements for exams, including invigilation. You can destroy these records one year after action is complete.

Note: This Disposal Schedule example does not mention any surveillance technology at all. Disposal Schedules are mostly format neutral. This means you can use 02.13.09 no matter what the format of the records. It applies to:

- online recordings from remote invigilation software and
- manual records made by a person watching an exam.

Disposal Schedule for the University of Tasmania (DA2398), 02.13.09.

Smart badges

Smart badges are a wearable technology. They use radio-frequency identification (RFID), near-frequency communication (NFC) or GPS.

Smart badges can:

- authenticate the wearer
- provide access to specific areas
- track time and attendance
- provide contact tracing and proximity detection
- send alerts.

Smart badges are worn at events, conferences and large warehouses. They are also worn at dangerous or remote workplaces like mines and construction sites.

Smart cards

Smart cards are the size of a credit card. They contain an integrated circuit (IC) chip that can process and store data.

Smart cards include:

- bank (credit or debit cards)
- identification (business or government identity cards)
- transport
- healthcare.

Public transport cards can store trip history and track individual's movements.

Smart city technologies

Smart cities use data and technology to improve quality of life, service delivery and sustainability.

Internet of Things (IoT) networks collect and send data from sensors and devices. Automation performs tasks with minimal human input. Artificial intelligence processes large amounts of data for data-driven decision making.

Smart cities focus on digital inclusion, energy, environment, infrastructure, safety, transport, urban planning and more. Examples of smart city technology include:

- CCTV, sensors, and number plate recognition that re-route traffic to ease congestion
- lampposts collect data about pedestrian traffic to create better footpaths and roads
- live video feeds from surveillance cameras use AI to identify incidents such as fights or vandalism, and send alerts to police
- rubbish bins send alerts to collectors when they are full
- sensors alert drivers to parking spaces through mobile apps
- smart solar benches equipped with charging ports and Wi-Fi.

Smart meters (digital meters or advanced meters)

Smart meters record live use and report regularly, for example, at five-to-thirty-minute intervals. Data is sent to the consumer and the utility company. The amount and frequency of data means companies may identify when household occupants are asleep or absent.

Although mainly used for electricity, gas and water smart meters also exist.

Example 11: Smart meters (Aurora Energy)

You can destroy meter reading data and billing calculations, bills issued for payment, reminder notices and final demands for payments seven years after action is complete.

Disposal Schedule for Aurora Energy (DA2509), 04.02.

Context: Other records about smart meters have different retentions:

- project management records (like final reports and recommendations) on introducing smart meters are permanent
- decisions to decommission technologies, such as traditional meters boards are permanent
- you can destroy communication, advertising or marketing campaign records ten years after action is complete.

Disposal Schedule for Aurora Energy (DA2509), 05.01, 05.01, 05.02.

Speed cameras (safety cameras)

Speed cameras started as fixed cameras in one place to detect speeding. They now include:

- hand-held cameras
- mobile speed cameras on trailers
- average (point to point) speed cameras.

Speed cameras work using sensors or radars. When vehicles go over the speed limit or run a red light, cameras activate and take a photo.

New speed cameras take photos to detect offences like illegal mobile phone use or not wearing a seat belt. Artificial intelligence analyses the photos. Automated Number Plate Recognition (ANPR) cameras can identify stolen or unregistered vehicles. They do this by cross-checking licence plates against databases.

Example 12: Speed cameras (Tasmania Police)

You can destroy speed camera images six months after action is complete where:

- no offence has been detected
- no infringement issued and
- no further police response is required.

Disposal Schedule for functional records of the Department of Police and Emergency Management (DA2351), 10.04.02.

Example 13: Speed cameras (Tasmania Police)

You can destroy road safety speed camera infringement notices seven years after action is complete.

Disposal Schedule for functional records of the Department of Police and Emergency Management (DA2351), 10.04.03.

Context: Different organisations have responsibilities for speed cameras and related records. For example:

- Tasmania Police issue infringements
- State Growth manage installation of traffic monitoring, speed and red-light cameras.

Other records related to speed cameras you need to keep include:

- road safety policy
- AI policy, implementation, testing, decisions, etc.
- placement of surveillance equipment, maintenance and checks
- privacy assessments.

Records may have different retention periods, from short-term to permanent. Records may be described in more than one schedule, including common schedules.

Disposal Schedule for common administrative functions (DA2157), *Disposal Schedule for short term value records* (DA2158), *Disposal Schedule for Transport Infrastructure and Services of Department of Infrastructure, Energy and Resources* (DS43).

Voice assistants (VA)

Voice-activated software interacts with users, performing requested tasks or services. Voice assistants are often integrated into smart phones and smart speakers.

Voice assistants can monitor, understand, and record speech. They can:

- send email or text messages
- make calls
- find information online
- schedule meetings
- play music
- manage smart home or office settings like lights or heating.

Wastewater surveillance

Wastewater surveillance tracks and monitors prevalence of infectious diseases in near-real time. Data can also identify hot spots of drug use and measure environmental contaminants. Results are used by:

- environmental protection and public health to assess potential environmental and health risks
- law enforcement and public health to develop drug and alcohol policies
- public health to respond to specific diseases through public awareness campaigns or vaccinations.

Wearable technologies (wearable tech)

Any technology designed to be worn. Examples include:

- activity trackers
- ankle bracelets
- body worn cameras
- smart glasses
- smart watches.

Workplace surveillance

These technologies monitor employee behaviour, health, performance and more. They include:

- Activity or health tracker apps or wearable technologies. Used as part of corporate wellness programmes, they may include biometrics, health data and location.
- Algorithms. Used to ‘nudge’ employees to preferred behaviours for business efficiency.
- Biometric data. Access to buildings, phones, and computers through fingerprint, facial or voice recognition.
- Body worn cameras. Worn in high-conflict jobs like police, security, parking inspectors. Used for security, as a crime deterrent and to capture evidence of incidents.
- CCTV. Used for security, to deter theft and to track behaviour.
- Gamification of work. Game-like practices with scores, rewards, rules, and penalties. Digital dashboards display employee or team progress to encourage competition between workers. Used to improve employee performance.
- GPS location tracking. Used for work, health, and safety purposes, often at remote, large, or dangerous work sites. Common in cars and in staff identification and security access cards.
- Monitoring software. Tracks phone calls and computer actions. Software can monitor applications, browsing history, emails, file downloads, keystrokes and mouse movements. Used to protect corporate information by flagging suspicious actions, for example, large downloads. Also used to gain evidence to discipline or dismiss employees.
- Prediction tools. Used as part of recruitment vetting. For example, online profiling and social media screening.
- Time and motion data. Can track output and activity.
- Time-stamp attendance. Tracks employee time at work.

Example 14: Workplace surveillance (disciplinary action)

You can destroy surveillance evidence of investigations of suspected misconduct and unproven charges two years after the last incident.

Evidence may come from many sources. For example, CCTV, biometric data (to access buildings) or GPS location data from fleet cars.

Disposal Schedule for common administrative functions (DA2157), 12.10.02.

Context: We will review *Disposal Schedule for common administrative functions* (DA2157) soon. Misconduct retention periods will increase.

You also need to keep records about introducing workplace surveillance. This may include:

- legal advice
- privacy and risk assessments
- new organisational policies and procedures
- training
- ordering hardware and software
- equipment maintenance.

Disposal Schedule for common administrative functions (DA2157).

WHERE CAN I GET HELP?

Contact your records team for organisation-specific advice.

The Office of the State Archivist provides whole-of-government policy, advice and support on information and records management. Visit our website for more information.

REFERENCES

Australia New Zealand Policing Advisory Agency (2013) *2013 Australia and New Zealand guidelines for digital imaging processes*, ANZPAA, 17 September 2013, accessed 7 April 2025.

Australian Digital Recordkeeping Initiative (2020) *Sustainable digital file formats for creating and using records*, ADRI, Version 1.0 April 2020, accessed 7 April 2025.

Office of the State Archivist (2024) *Information and records management standard*, OSA, Version 1.1 29 May 2024, accessed 7 April 2025.

Office of the State Archivist (n.d.) *Retention and Disposal Schedules*, OSA, accessed 7 April 2025.

MORE INFORMATION

Office of the Victorian Information Commissioner (2022) *Guiding principles for surveillance*, OVIC, May 2022, accessed 7 April 2025.

Queensland Government (2021) *Digital images, audio and video*, Queensland Government, 9 July 2021, accessed 7 April 2025.

Queensland Government (2021) *Surveillance and monitoring records*, Queensland Government, 21 May 2021, accessed 7 April 2025.

CONTACT US

Office of the State Archivist | www.osa.tas.gov.au | enquiries@osa.tas.gov.au | 03 6165 5581

Records from surveillance technologies is part of the *Tasmanian Government Information Management Framework.* It supports the *Information and records management standard.* This is a living document and we will make minor changes as needed. If you notice anything that needs updating, please let us know.

License URL: www.creativecommons.org/licenses/by/4.0/legalcode
Please give attribution to: © State of Tasmania, 2025.

Document Development History

Version	Date	Comments
1	7/04/2025	Initial release