Information management: Digital disposal policy

Table of Contents

Policy statement and principles

What

This policy provides direction and guidance on the disposal of digital information held in Police operational and corporate systems.

Following the correct disposal practice enables Police to discharge its obligations under the Public Records Act 2005, using a defensible, repeatable process across the organisation's information systems.

The requirements in this policy are mandatory for the retention and disposal of all digital information and records held by Police and align with the overarching requirement to dispose of records in the Information Management Policy.

It is recognised that all Police systems are not yet enabled to meet these requirements, but this policy provides a pathway to achieving compliance. Compliance is expected to be achieved over time, and owners of Police systems must consider the requirements in this policy as they move through their normal process of upgrading and replacing the systems they manage.

Why

The final activity in the lifecycle of information is its disposal. Carrying out regular disposal enables easier discovery and collaboration, keeping Police compliant with information and privacy legislation.

This also helps Police to:

- locate and protect our high value, high risk information
- improve control over the collection, storage and management of our information
- reduce the risk of accidental or illegal disposal
- reduce the risk of privacy or security breaches
- minimise the possibility of 'over-disclosure' of information that could have been destroyed
- reduce ongoing storage costs
- meet our legislative and regulatory obligations
- comply with business agreements and contractual requirements.

The key legislation defining digital disposal (Destruction or Transfer to Archives New Zealand) is the Public Records Act 2005. This covers all records and information held by Police and requires that all disposal is executed in accordance with the Police Disposal Authority (DA648) and the General Disposal Authorities (GDAs) (approved by the Chief Archivist).

The Police Retention and Disposal Schedule (RDS) (part of DA648) is made up of Police's functions and activities, documenting how long the information will have value to Police (use, criticality), the minimum length of time the information must be retained, and what will happen to that information when it reaches its disposal timeframe - either destruction or transfer to Archives New Zealand.

The GDAs document functions that cover general organisational business activities such as financial management, human resources, and Ministerial activities carried out by most public offices.

Other legislation can have an impact on disposal, primarily by imposing maximum timeframes that Police can retain certain types of information, these include:

- Contract and Commercial Law Act 2017
- Criminal Procedure Act 2011
- Evidence Act 2006
- Policing Act 2008
- Privacy Act 2020

How

Digital disposal must follow a consistent, trustworthy process that meets the requirements of Archives New Zealand's Information and records management standard. That standard is reflected in this policy.

Disposal should be a function built into Police information systems, and not an action that is only taken once systems are no longer

required.

To carry out disposal, systems must have the capability to:

- apply the Police Retention & Disposal Schedule and Archives New Zealand's GDAs to information
- capture the correct metadata to enable disposal
- have a process to authorise disposal
- have a process to action disposal.

Most often, the mechanism to enable routine, scalable disposal will be workflow. A workflow will ensure each stage of the process is complete before moving to the next stage, e.g. the system will ensure disposal has been authorised at the appropriate business level, before carrying out any disposal action.

Following a consistent process will ensure that Police can dispose of material systematically at scale and will also deliver an auditable process for review and modification when required.

See Appendix 2 - Digital disposal workflow.

Archiving vs Disposal

Archiving and disposal are two different actions that can occur over information.

- **Disposal** is the final and irreversible action over information.
- **Archiving** is the movement or migration of information, usually to other storage.

When information is disposed of it is destroyed, and no longer in Police's control. Disposal can also be the transfer of information to another agency, such as Archives New Zealand.

While the term 'archiving' may be used in place of disposal, these are two different and separate activities. Within organisations, when material is referred to as having been 'archived' this means it has not been destroyed but may have been moved or migrated to lower tier or less expensive storage. Police still control the information.

Scope

This policy applies to:

- all Police employees (whether permanent or temporary) and contractors and volunteers
- all business activities performed by or on behalf of Police
- all information and records relating to those business activities regardless of format
- all systems that hold records and information at Police.

This policy does not apply to:

- system back-ups of information, records and their associated data - these exist for a limited period of time and are not part of the digital disposal process; their retention is for disaster planning and other unexpected events. They are retained in line with GDA 6/Class 8.1.1 (Retain for the active life of the system/Destroy).

Definitions

Aggregations of information	A collection of information about a Police function or activity. This allows the bulk application of a disposal class to all the information within the aggregation, i.e., a digital case file, a physical HR file, a collection of evidence event.
Archiving	The movement or migration of information, usually to other storage. **Note:** While the term 'archiving' may be used in place of 'disposal', these are two different and separate activities. Within organisations when material is referred to as having been 'archived' it usually has not been destroyed but may have been moved or migrated to lower tier or less expensive storage. Police still control the information.

Data/Data elements	A specific piece of data within a data series or set (e.g. the address of a specific firearms license holder).
Data series/table	A data series is a collection of data within a dataset that has a defined purpose (e.g. Firearms license holders' addresses).
Dataset	A dataset is a collection of related, discrete items of related data that may be accessed individually or in combination or managed as a whole entity. (e.g. Firearms license holders).
Disposal	Disposal is the final and irreversible action over information. This may be its destruction (whether from a digital system, as a physical file or as a media object) or its transfer to another agency i.e. Archives New Zealand. Post transfer Police no longer have control of the information so it is considered to have been disposed of.
Disposal Authority	The instrument used by Police that defines the disposal actions that has been authorised for specific records.
Disposal Class	A category defined in the Disposal Authority that describes the activity that is covered, the minimum time the information must be retained, provides a disposal trigger (the event from which the disposal date is calculated), and the disposal action that will take place.
Information	A blanket term that refers to anything created or used by Police in the conduct of our business, regardless of format.
Metadata	The information that helps people to find, understand, authenticate, trust, use and manage information and records. If information and records have metadata, we know what it is, what it has been used for, and how to use it. Metadata also makes information and records easier to find.
Records	Records are information, whether in its original form or otherwise, including (without limitation) a document, signature, a seal, text, images, sound, speech, or data compiled, recorded or stored as the case may be: 1. In written form or any material; or 2. On film, negative, tape, or other medium so as to be capable of being reproduced; or 3. By means of any recording device or process. Records have been created or collected into a meaningful form containing context and content regardless of format. Under the Public Records Act Police is required to keep records for a period of time as evidence of its transactions and outputs.
Retention and Disposal Schedule (RDS)	The part of a Disposal Authority listing the specific minimum retention periods for different records classes and the disposal actions that should occur when the information is ready for disposal.
Retention period	The minimum length of time after the disposal trigger commences that a record must be maintained and accessible. At the expiration of the retention period, a record may be subject to a disposal action or to further review if the record is determined to still have business value to Police.
Systems/Information systems	An organised collection of hardware, software, and other elements which stores, processes, and provides access to an organisation's business information and data.
Transfer	The process of re-assigning the ownership of records to another agency (e.g. Archives New Zealand or another government agency when a function transfer occurs).

Principles

A robust digital disposal practice follows these principles:

- **Disposal is part of system design** - It is a functional and fundamental requirement of Police information systems. Without an efficient way to apply disposal, it is a labour-intensive and inefficient activity, prone to error.

- **Disposal is a regular, on-going activity** - In order to keep systems compliant, uncluttered and up-to-date, disposal should be a 'business as usual' activity.
- **Disposal is authorised at the correct level** - Authorisation for disposal will usually be the Information Asset Owner or other tier 3, 4 or 5 manager, although the disposal operation may be carried out by the Information Asset Custodian or similar role.
- **Disposal is lawful** - Authorisation is carried out in accordance with regulatory, legislative and business requirements and agreements.
- **Disposal metadata is retained** - the appropriate disposal metadata must be collected and retained in accordance with Archives New Zealand's Minimum requirements for metadata. (Appendix 1)
- **Disposal is format agnostic** - information and records in all formats are covered for disposal.
- **Disposal is permanent** - post disposal, information cannot be reconstructed.

Metadata

The appropriate collection of metadata is vital to enable identification of information for disposal and to retain a record of disposal post destruction/transfer.

Under the Public Records Act, Police are required to only dispose of information once it meets its approved disposal criteria and timeframe (as outlined in Police's Disposal Schedule and the GDAs). In digital systems, the specific criteria around disposal activities is captured and actioned via metadata. This is defined in Police's Metadata Standard which outlines the specific metadata that must be generated and maintained for disposal actions (see also Appendix 1).

This also aligns with the minimum metadata set required to be captured and retained when records and information are created and disposed of.

Digital disposal process

All disposal follows the same practice regardless of format, but processes may differ dependent on the capabilities of each system and linkages between them.

This policy recognises that some systems that hold information at Police are connected in complex ways. While the requirements below apply to all systems that hold information, some individual systems may meet these requirements by demonstrating that the information they hold is managed and controlled in other systems.

Assign class

All information and records to be disposed of must have a disposal class applied to them under the Police Disposal Authority or the GDAs.

- The system must be enabled to apply disposal classes to aggregations of information and records.
- The system must apply classes to aggregations of information as early as possible, ideally at the point of creation.
- The system must be capable of assigning a temporary classification/tag/label to aggregations of information when no disposal class exists (e.g. a new business activity not yet covered in a Disposal Authority).

No disposal can occur over information and records when no disposal can be determined.

Monitor

Although the disposal process follows a comprehensive, auditable workflow, systems must be regularly monitored to ensure:

- aggregations of information are correctly having the appropriate disposal classes applied
- disposal workflows are operating as required
- systematic review of approvers/authorisers for disposal occurs.

Authorise

Information being disposed of must be approved for disposal at the appropriate responsibility level at Police before any disposal action occurs.

The authorisation process requires approval by the Information Asset Owner or other tier 3, 4 or 5 manager.

When information has met its retention period, before any disposal takes place, it must be reviewed for any further business need to retain, this includes other uses the information may have been put to. For example, information may have been used for a prosecution and has now met its disposal timeframe but is still being utilised by another business unit for intelligence purposes.

The retention period in Disposal Schedules is the minimum period information must be retained. Except in a few cases, the Police RDS does not prescribe the maximum length of time information should be retained.

However, information should only be retained longer than a retention period if Police has a legitimate business reason to do so. For example:

- an investigation / incident file has not completed

- the information is still in use, has ongoing business value to Police, and there are no other legislative or legal requirements mandating its disposal
- the information is the subject of an active Official Information Act / Privacy Act request
- the information is the subject of a judicial, criminal or other review or appeal. The information falls within an all of government disposal moratorium relating to specific types of information, e.g. *Royal Commission of Inquiry into Historical Abuse in State Care & Faith-based Institutions (Royal Commission)*
- the information holds historic significance and meets the criteria to be retained by the Police Museum.

In circumstances where legislation creates overlapping or conflicting retention periods:

- the longest retention period applies. This includes situations where material is covered by more than one disposal class
- where there is a conflict advice should be sought from Police Legal and the Information Capability team on the correct retention period to use
- where other legislation requires that Police do not hold information beyond a certain time frame- disposal must take place once those timeframes are reached.

See Appendix 3 - Disposal decision process.

In cases where the disposal is not authorised (it is determined to retain the information), a system must be capable of extending a disposal period to allow for future review and to continue to secure, store and manage information until disposal is authorised.

Dispose

When information and records are ready for disposal (once authorisation has occurred), a system must take disposal actions.

A system must:

- employ a method of disposal that is permanent - material cannot be reconstructed
- be enabled with the requisite capability for digital transfer if material is required to be transferred to Archives New Zealand.

Report

A system must be able to demonstrate that the disposal activity occurred within a lawful, legal framework. System reporting provides a record of Police's past actions and decision-making - retaining a history of the disposal activity over the information allows Police to respond to any future questions and requests for information.

For this reason, the system must be enabled to generate the requisite disposal metadata to show what has been disposed of, and that disposal has occurred.

Note that records of these disposal decisions are themselves required to be retained for 10 years from the date of the disposal action (GDA 6/class 8.1.3).

Disposal of data

Due to their dynamic and changing properties, datasets and their data need a considered approach to their disposal. Their use and ongoing value will be the criteria considered when applying disposal criteria. Unlike other static information, datasets will experience ongoing growth and change, making disposal decisions more complex.

Principles

Regardless of the disposal approach(es) used, the following principles apply to the disposal of data/sets:

- **Disposal of data with more than one disposal class** - The data will be disposed of in accordance with the disposal class carrying the longest retention period.
- **Disposal of non-mastered data** - Where data in a dataset is mastered in another dataset, the non-mastered instance will be disposed of as a duplicate in accordance with General Disposal Authority 7 (GDA 7).
- **Disposal according to (non-PRA) legislative requirements** - Where other legislation requires that Police do not hold data beyond a certain point - disposal must take place once those timeframes are reached.
- **Disposal of data/data series/datasets with conflicting legislative requirements** - In circumstances where the Police RDS and other legislation and agreements dictate differing minimum/maximum retention periods, this will be discussed and resolved with Police Legal and the Information Capability team.

Disposal approaches for data

While the five steps in the disposal process should still be followed, the owner of a dataset should determine which of the following three approaches is appropriate for their data and document the disposal approach alongside other information about the maintenance of the dataset. In some cases, more than one of the approaches can be used where specific data elements require a different approach to the majority of a dataset.

- **Disposal of the entire dataset at end of life** - An entire dataset can be disposed of when it is no longer in use. There may be one or more disposal classes applied to the entire dataset if parts of the dataset have been used for different activities carrying different disposal classes.
- **Disposal of individual data series/tables** - In cases where parts of a data set are no longer being used/collected or required for analysis, then those groupings can be disposed of separate to the rest of the dataset. Care should be taken to ensure that removing parts of a dataset this way does not affect the integrity of the data set overall.
- **Disposal of data elements based on age or other criteria** - For cases where specific data elements are expired, inaccurate or no longer relevant, disposal can take place at the data element level. Examples of when this will be appropriate include:
    - bad or inaccurate data that needs to be cleansed from a dataset
    - data that can no longer be retained due to privacy or other legislative requirements
    - data over a certain age that no longer has value for analysis
    - data mastered in other systems that is no longer required.

The owner of the dataset should also be cognizant of other business uses that the data may be utilised for by others when deciding which disposal approach/es should be applied.

Other digital disposal scenarios

While the majority of digital disposal should take place within systems using the steps outlined above, the following exceptions can occur:

Disposal of information held in more than one system

Information at Police can be duplicated or held in multiple systems. Information can be shared between systems, copies can be made, or systems may actively share information between themselves in real-time.

When considering disposal of information held in multiple systems the following principles apply:

- If information held in a system can be clearly identified as a duplicate and is **being used for the same purpose/function as the 'master'** instance of that information, then duplicates can be disposed of with less rigor using GDA 7 (see note below).
- Where duplicate information is being held in multiple systems, but is **being used for different purposes**, then each instance of the information must be treated separately for the purposes of disposal.

- Where information in a system (a) can be clearly identified as **having its disposal take place in another system** (b), then the first system (a) is not responsible for disposal of the information.

Disposal of information held in systems not configured for disposal

It is recognised that some older systems will not be enabled with workflow to support disposal and will require an ad hoc disposal process.

In these cases, the following high-level process should be followed:

- identify the information and records requiring disposal
- describe the information with enough detail to allow the application of disposal classes
- apply disposal classes
- carry out a review of the information to ensure it is ready for disposal
- extract information for disposal
- dispose of the information
- capture the minimum metadata required for reporting purposes.

In all cases, the Police Information Management team function should be involved in the above process to ensure it is compliant.

The above process also applies when Police information systems are being decommissioned.

Disposal of information held on hosted/external systems or systems 'shared' between entities

Where Police information is held on systems not owned or managed by Police, the requirements of this policy still apply. Contracts/agreements for these systems should clearly specify what happens to police data/metadata when a contract ends, to ensure disposal can take place.

Where Police information is shared between public agencies, and held on other agencies' systems, the agreement or MOU between the agencies must stipulate who is responsible for disposal of information in the shared system, and what will occur when information held in a shared system has different agency disposal requirements.

Disposal under General Disposal Authority 7 (GDA 7)

Disposals under GDA 7- Facilitative, transitory and/or short-term value records **do not have to be recorded**. This class describes low-level, short-term value information and exists to allow the normal administrative removal of information such as low-level working notes, preliminary drafts, duplicate material and early versions of information.

Responsibilities

Not everyone at Police will be involved in the digital disposal process, but as information stewards we all have a part to play in ensuring that we create full and accurate records and store them in the appropriate systems. This enables the application of disposal classes to information, a prerequisite for digital disposal.

Role	Responsibility
All users	- Create full and accurate records, storing them in the appropriate corporate or operational system. - Do not dispose of records without the appropriate authorisation.
Information Asset Owner / Information system business owner	- Accountable for an information asset or set of assets. - Accountable for any disposal operations carried out. - Accountable for ensuring that the correct disposal metadata is collected.
*Information Asset Custodian / Information system administrator	As the administrator of the system: - Carries out the disposal action following authorisation from the Information Asset Owner. - Supports the Information Asset Owner in the disposal process.
Manager, Information Capability	- Supports Information Asset Owners and Custodians in the disposal process as needed. - Liaise with ICT as needed for any assistance required.
ICT Product Managers/Owners	- Assist Information Asset Owners/Custodians and systems owners with configuration of systems to enable disposal.

*For some systems, particularly smaller systems with a single line of business or discrete collections, the Information Asset Owner and the Information Asset Custodian may be the same person, carrying out dual roles.

Appendix 1 - Archives New Zealand's metadata requirements

Minimum data to assign when creating and managing information and records

- Unique identifier
- Name
- Date created
- Business activity documented
- Creator (person or system)
- Name and version of the software application used to create or document a record
- Any later actions carried out on the record, such as accessing, modifying or disposing
- Identification of the persons or systems carrying out those later actions
- Dates those actions were carried out

Minimum metadata to assign when disposing of information and records

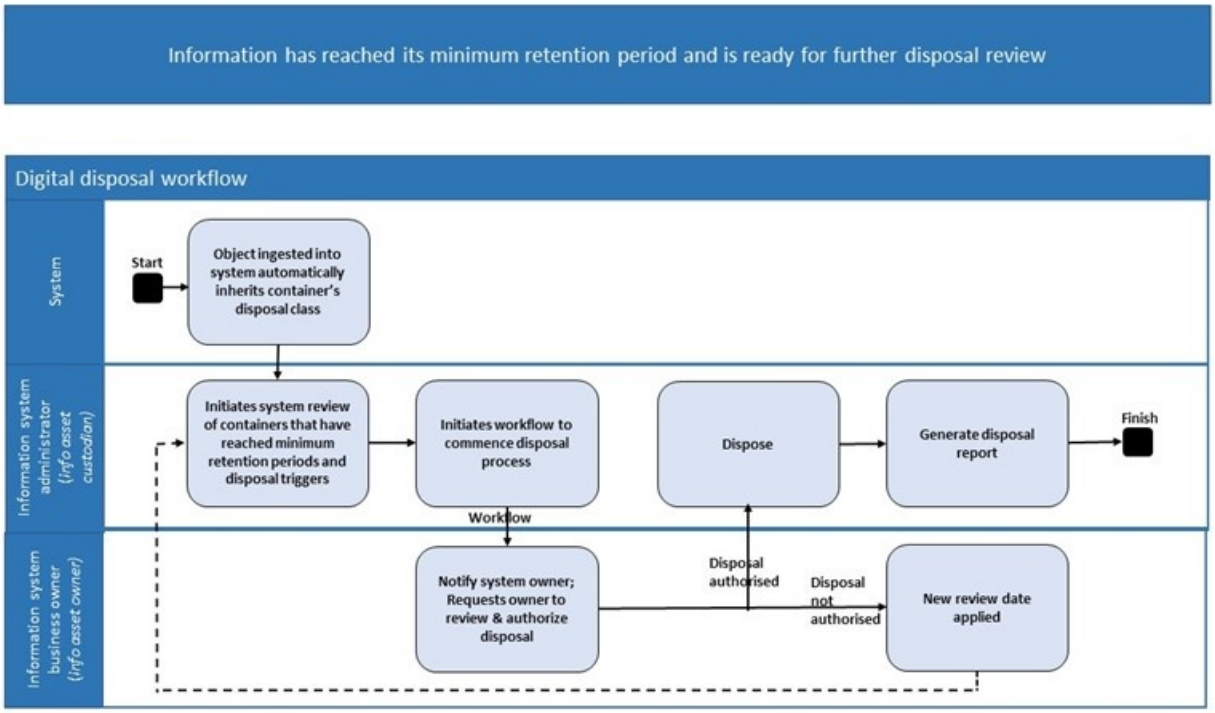
- Unique identifier
- Name
- Date created
- Business activity documented
- Creator (person or system)
- Date of disposal
- Authority governing the disposal
- Person or role carrying out the disposal action

Police may need to assign further metadata to:

- Ensure that the record is full and accurate
- Establish a complete context
- Prove authenticity

These metadata fields are further defined in Police's Metadata Standard.

Appendix 2 - Digital disposal workflow



Appendix 3 - Disposal decision process