Information Management: Policy and guidelines for the storage of physical files

Table of Contents

Policy statement

What

This chapter sets out requirements for storage of physical files (including digital files held on removable media such as CDs and DVDs) so as to ensure physical files are:

- identifiable, retrievable, accessible and usable for as long as they are required
- protected from unauthorised or unlawful access, alteration, loss, deletion and/or destruction
- actively managed to ensure they are not retained longer than is required.

It also provides guidelines for the onsite and offsite storage of physical files. Where the decision is taken to store physical files offsite, it requires those files to be stored with Police's official offsite storage provider, 'The Information Management Group' (TIMG), in one of its secure storage facilities.

It proceeds on the assumption that most information is now being created or received electronically, and that information and file management will increasingly focus on managing digital rather than physical files. The number of physical files being created will continue to reduce. This assumption is already being factored into the development of new Police stations which have less space allocated for physical file storage.

This chapter applies to all Police employees, whether permanent or temporary, and includes contractors and volunteers.

Why

Security and storage arrangements must allow employees to control Police physical files and maintain their integrity for as long as required. Maintaining the integrity of physical files means protecting them from alteration, damage or destruction, whether intentional or unintentional, preventing their deterioration, and ensuring they remain usable. Inadequate storage conditions or inappropriate handling practices can compromise the integrity of files.

TIMG provides secure off-site storage and a records destruction service to Police (managed by the Police National Procurement Group) and many other agencies under a syndicated procurement agreement. TIMG has the facilities to store our files safely and securely to the required standard. It reports quarterly to the Police National Procurement Group detailing all file activity, including secure destruction, and reporting against agreed KPIs, in particular relating to timeliness and any significant deviations from expected volumes. Where there is an assessed need to store physical files offsite, the services of TIMG should be used.

Active lifecycle management of physical files is essential in terms of minimising storage costs and ensuring efficient use of limited space. Prompt processing of physical files after closure will promote a manageable flow of files for both onsite and offsite storage and also for disposal. Files should be retained only for their designated retention period.

How

Police will store physical files in accordance with the six storage requirements set out in this chapter. These six requirements reflect, in more detail, requirements 2.4, 3.3 and 3.4 of the Information and Records Management Standard, insofar as those requirements relate to physical information and records. This is a mandatory standard issued by the Chief Archivist under section 27 of the Public Records Act 2005.

Storage requirements for physical files

Requirement 1 - Files must be secure

Assess security risks to physical files and plan and implement protective security arrangements for them.

- In an office environment, files with a national security classification of SENSITIVE or RESTRICTED should be held in a lockable storage area or cabinet.
- In any onsite storage facility, all files (including those with a classification of IN CONFIDENCE) should be protected through controlled access to the storage areas, and through a secure physical environment.

Requirement 2 - Files must be protected from natural and man-made hazards

Choose suitable locations for physical files. Assess and reduce the risks of damage and destruction to physical files. Take into account:

- general environmental factors - light, heat, humidity, dust, pollutants, insects, rodents, mould, power outages;
- building location - vulnerability to floods, earthquakes, fires and volcanic eruptions;
- location in building - vulnerability to flammable finishes or furnishings, chemicals, water leaks, and electromagnetic interference generated by power plants, elevator shafts, power cables and lightning conductors.

Requirement 3 - At-risk files must be identified and managed appropriately

Promote awareness of files with long-term value, files older than 25 years, and files stored close to hazards or in other sub-optimal conditions. Take action to reduce or eliminate significant risks to the integrity of these files (see Requirement 5).

Requirement 4 - Files (including digital files held on removable media) must be stored in conditions that ensure their safe care and custody

These files must be:

- stored in buildings with fire protection systems and equipment compliant with the New Zealand Building Code;
- stored above floor-level using shelving or equipment that is seismically restrained (where required) and appropriate to the format of the records or the size of the storage media;
- stored away from, or otherwise protected from, sunlight and artificial light;
- stored away from magnetic interference, if they are digital records held on removable media;
- arranged in an orderly manner; and
- retrieved, handled and re-shelved in accordance with set procedures.

Requirement 5 - Inactivated or closed files (including inactivated or closed digital files held on removable media) must be identified and stored in a dedicated storage area

Storing inactivated and closed files in a suitable storage area, such as a sole-purpose room or with TIMG, will:

- make it easier to manage records through to disposal;
- reduce the risk of losing records;
- improve the security of records;
- make it easier to manage environmental hazards.

Requirement 6 - Dedicated storage areas for inactivated or closed files (including inactivated or closed digital files held on removable media) must ensure the preservation of those records in a usable form

These storage areas must:

- be located in buildings which comply with the provisions of the New Zealand Building Code in force at time of construction and with any associated codes and standards;
- have adequate floor loading capacity and shelving that is seismically restrained, where required;
- have drainage systems adequate to prevent flooding or must be located in buildings with drainage systems adequate to prevent flooding;

- be insulated from the outside climate;
- be protected from internal hazards;
- be maintained over time in accordance with a documented maintenance programme;
- be intruder resistant and have an alarm system or be located within buildings that are intruder resistant and have an alarm system; and
- be kept clean and free of pests such as rodents and insects.

Responsibilities

Roles and responsibilities associated with the storage of physical files are set out in this table.

Role	Responsibility
Manager Information and Knowledge	Implements monitoring and auditing processes for regular assessment of performance against this chapter.
District Commanders /Directors	Ensure adequate resources are made available to implement this chapter within their district or area of national responsibility.
District File Management Staff	Manage the storage of records within the station, for off-site storage and for disposal, in accordance with this chapter and the Police Retention and Disposal Schedule.
PNHQ File Management Staff	Manage PNHQ records for off-site storage and for disposal, in accordance with this chapter and the Police Retention and Disposal Schedule.
Managers	- Ensure their employees are aware of this chapter and know their responsibilities under it. - Ensure their employees are supported and their performance is monitored in relation to compliance with this chapter.
Person in charge of an active file	- Ensures it is stored in accordance with the storage requirements in this chapter. - Once the file is closed or inactivated, ensures the relevant action is taken to file it. - Seeks assistance from records staff when unsure about any aspect of his or her responsibilities under this chapter.

Where to store - onsite or offsite?

There are several factors that need to be taken into account when deciding the optimal mix of onsite and offsite storage for physical files.

- **Active** physical files need to be stored onsite for ready access and active file management.
- **Inactivated** physical files can be retained at stations but need to be regularly reviewed and eventually closed according to established criteria.
- **Closed** physical files are sent to File Management Centres (FMCs) for filing, and will be either retained onsite or sent offsite. At PNHQ business units send their closed physical files to PNHQ File Management for offsite storage.

There are clear benefits in regularly reviewing space allocation for onsite physical file storage in light of changing operational requirements. Assuming a changing focus to digital as opposed to physical file management, the expectation should be that over time, less space will be required for physical file storage.

The key determinants for retaining files onsite at the FMCs will be the availability of compliant storage space and overall storage costs.

- **Insufficient compliant storage space onsite** - Where there is insufficient space onsite that complies with the storage requirements set out in this chapter, then the cost of becoming and remaining compliant will need to be weighed against the cost of storing offsite with TIMG in one of their compliant facilities, and against any competing requirements for space.
- **File retention periods** and disposal actions are also relevant. For example, files that are marked for destruction after 3 years could be retained onsite if they are regularly processed for destruction and volumes remain fairly constant. Unless they can be accommodated onsite, files that need to be retained for 5 or 10 years or longer should be stored offsite.