

## **Part 5 - Carrying out search powers with or without warrants**

## Table of Contents

Table of Contents	2
Policy statement and principles	4
What	4
Why	4
How	4
Powers incidental to search	5
Police actions authorised by search powers	5
Powers when conducting remote access searches	5
Limitations on exercising search powers	5
Using assistants during searches	6
Powers of persons called to assist	6
Powers of persons called to assist remote access search	6
Powers of constables who assist	6
Special powers when an application for search warrant is pending	6
Powers of detention incidental to searches of places and vehicles	6
Determining a connection	7
Detention for the shortest period practicable	7
Powers to search persons at a place or vehicle	7
Powers of search when suspect pursued	7
Risk assessment when planning searches	8
Maximising safety and minimising risk	8
Planning searches of places, vehicles or things	8
Required risk assessments for searches	8
Conducting your risk assessments	8
Additional risk assessments for search warrants	8
Urgent situations and re-assessing change	8
Planned Action Risk Assessment and CARD Prompt, and 'OnDuty Noting'	8
Do not disclose planned action risk assessment without advice	9
Procedure for planning searches	10
Planning for searches	10
Examples of risks associated with searches	11
Safety options to mitigate search risks	12
Separating individuals posing risk from premises to be searched	14
Tactical arrest or interception in public place	14
Planning to separate individuals from premises	14
Execution of searches and mandatory notifications to COMMS and DCCs	15
Notification procedures to COMMS and DCCs	15
Warrantless searches	15
Executing search warrants	15
Covert searches	16
COMMS and DCCs responsibilities	16
Steps to follow after execution phase	16
Entry, announcement and identification requirements	18
Powers of entry	18
Search warrants to enter and search vehicles	18
Identification and announcement requirements on entry	18
Exceptions to announcing entry and giving reasons for the search	18
Securing the scene to be searched	19
Case Law	19
Using force on entry and detaining people at the scene	19
Being "in uniform"	19
Use of force against persons and property	20
Using reasonable force to enter property	20
Announced forced entry	20
Unannounced forced entry	20

Entry with firearms	20
Ensuring the safety of Police and others	20
Detaining people at searches of places or vehicles	21
Options prior to using force on a person	21
<b>What can be searched and seized?</b>	<b>22</b>
What can you search?	22
Searching people at the scene	22
What can you seize during the search?	22
Items of uncertain status	22
Case law	22
Seizure of items in plain view	23
Case Law Roskam v R [2019] NZCA	23
Case law: Smith v Police [2019] NZHC 2111	23
Seizing privileged materials	23
<b>Searching for and seizing computer material</b>	<b>24</b>
What computer material can be searched and seized?	24
Intangible material on, or accessible from cell phones or computers	24
Definitions related to computers	24
Search of a computer under warrant	25
Search of a computer without warrant	25
Carrying out a search of a computer	25
Carrying out a search of a cell phone	26
Extraction process used to retrieve intangible data from cell phones	26
Remote access searches authorised by warrants	27
Additional powers when conducting remote access searches	27
Principles for data evidence gathering	27
Procedures for accessing computers, securing evidence and creating forensic copies	28
Securing evidence	28
Disposal of forensic copies	28
Information tending to incriminate	28
Privilege and confidentiality	29
<b>Cloud computing</b>	<b>30</b>
Information in the cloud	30
Advantages and disadvantages of cloud computing	30
How to get information out of 'The Cloud'	31
<b>Notice and inventory requirements after search or seizure</b>	<b>32</b>
Notice requirements	32
Form of written notice when exercising a search power	32
Case Law	34
Postponing compliance with notice and inventory requirements of items seized	34
Procedure for recording seized items and providing required notice	34
Limits on who can be treated as occupiers or people in charge	35
Notice requirements for remote access search	35
Duty to give notice to owners of things that are seized	35
Notice and inventory requirements relating to production orders	36
Procedure when seizing items for non-payment of fines	36
Further information	36
<b>Postponing compliance with notice requirements</b>	<b>37</b>
Application to postpone compliance with providing notices	37
Timeframes	37
Application for further postponement or dispensation	37
Restrictions on postponing compliance relating to seized things	37
<b>Search warrants, production orders and examination orders involving media organisations</b>	<b>38</b>
Background	38
Procedural guidelines (search warrants, production orders and examination orders)	38
Notice to Crown Prosecutor	39
Protection of journalists' sources	39

## Policy statement and principles

### What

The [Search and Surveillance Act 2012](#) brings together most Police and law enforcement search, seizure, surveillance and related powers. The Act sets out detailed rights, powers and obligations in relation to exercising those powers. The powers in the Act are designed to make it easier to detect and apprehend offenders committing serious criminal offences.

This part of the [Search](#) chapter details procedures for Police employees carrying out search powers with or without warrant and provides guidance on associated rights, powers and obligations that arise when searching places, vehicles or things.

Searches by way of warrant or warrantless powers have inherent safety risks and because of their intrusive nature have the potential to cause harm to Police employees and the public. Police employees planning and undertaking searches must therefore mitigate these risks as much as possible while enforcing the law.

### Why

Key functions of the Police are law enforcement, crime prevention and the maintenance of public safety. As an employer, Police has a responsibility to ensure that its employees are safe when they undertake their duties.

Compliance with the guidance and procedures in this chapter when carrying out search powers will:

- ensure compliance with the [Search and Surveillance Act](#), and other enactments like the New Zealand Bill of Rights Act 1990
- maximise safety and eliminate or minimise the potential harm that executing a search warrant or exercising a search power may have
- increase the chance of successful prosecutions.

### How

To meet its objectives and obligations when carrying out searches with or without warrants, Police will:

- ensure it has a lawful authority to search and exercise any other incidental power in relation to that search, including the use of force
- conduct risk assessments when planning searches and take action to mitigate risks to protect the safety of the public and of staff carrying out the search
- only seize what it is lawfully entitled to seize
- provide appropriate announcements and identification on entry
- satisfy the notice and inventory requirements detailed in the Act after search or seizure.

**Note:** Searches of persons subsequent to arrest, are not covered in this chapter.

## Powers incidental to search

### Police actions authorised by search powers

Every search power (with or without a warrant) authorises you to:

Action	You may...
Enter and search	Enter and search the place, vehicle, or other thing you are authorised to enter and search, and any item(s) found in that place, vehicle or other thing.  You can do this at any reasonable time.
Request assistance	Request assistance from any person with the entry and search (including a member of a hapū or an iwi if the place to be entered is of cultural or spiritual significance to that hapū or iwi).
Use reasonable force in respect of property only	Use reasonable force on property only to carry out the search and lawful seizure.  <b>Note:</b> This power does <b>not</b> authorise the application of force to any person (s115(3)). (Section 125 covers use of force against a person for search purposes - see <a href="#">Searching people</a> ).
Seize	Seize anything that is the subject of the search or anything else that may be lawfully seized.  See <a href="#">What can be searched and seized</a> in this chapter for more information.
Bring and use equipment	Bring and use any equipment or use any equipment found on the place, vehicle or other thing.  You may also use electricity from the place, vehicle, or other thing to operate equipment that it is reasonable to use in the circumstances for the entry and search.
Bring and use dog	Bring and use a trained law enforcement dog and its handler in or on the place, vehicle, or other thing being searched.
Copy documents	Copy any document, or part of a document, that may lawfully be seized.
Access a computer system or other data storage device	Use reasonable measures to access a computer system or other data storage device located (wholly or in part) at the place, vehicle or other thing if any intangible material that is the subject of the search may be in that computer system or device.
Copy intangible material	Copy intangible material accessed as above or which may otherwise be lawfully seized. This includes previewing, cloning, or using other forensic methods before or after removal for examination. See <a href="#">Searching for and seizing computer material</a> in this chapter for more information.
Take photographs, and recordings	Take photographs, sound and video recordings, and drawings of the place, vehicle, or other thing being searched and anything found there, <b>if</b> you have reasonable grounds to <b>believe</b> they may be relevant to the purposes of the entry and search.

(s110)

### Powers when conducting remote access searches

If you are executing a search warrant authorising a remote access search, you may:

- use reasonable measures to gain access to the thing to be searched
- copy intangible material in the thing being searched or that may otherwise be lawfully seized (this includes previewing, cloning, or other forensic methods).

(s111)

### Limitations on exercising search powers

The search powers listed [above](#) are subject to:

- any conditions imposed by an issuing officer when issuing a search warrant
- the privilege and confidentiality provisions in the Act.  
(s [115](#))

They are also subject to the requirements of "reasonableness" under section 21 New Zealand Bill of Rights Act 1990.

## Using assistants during searches

If you call on a person to assist you to exercise a search power, or a person has been required to assist you as a condition of a warrant, they are subject to your control and the overall responsibility for exercising the power rests with you.

You must, (unless they are another constable):

- accompany them when they first enter the place, vehicle, or other thing to be searched, and
- provide reasonable supervision of them.  
(s [113](#))

## Powers of persons called to assist

Any person called to assist you exercise a search power may enter the place, vehicle or other thing to be searched, but can only exercise the power of assistance and other powers listed in the table [above](#) as directed by you. For example, an assistant can only search places you determine are lawful to search, take photographs, or bring in and use equipment or electricity that you determine may lawfully be taken or used.

(s [113](#))

## Powers of persons called to assist remote access search

A person called to assist you execute a search warrant authorising a remote access search, has the same powers as you to:

- use reasonable measures to access the thing to be searched
- copy intangible material that is the subject of the search or that can be lawfully seized.

However, they can only exercise these powers under your control and supervision.

(s [114](#))

## Powers of constables who assist

Other constables assisting you with searches may exercise any power ordinarily exercisable by them, without direction or supervision from you.

## Special powers when an application for search warrant is pending

See Part 2- [Search warrants](#) for information about your power to enter and secure a place, vehicle or other thing when a search warrant application is about to be made or is awaiting the issuing officer's decision.

## Powers of detention incidental to searches of places and vehicles

If you are exercising a search power in relation to a place or vehicle, you (or a person assisting you) may **detain** any person to determine whether there is a connection between them and the object of the search if the person:

- was there at the start of the search, or
- arrives at the place or stops at, or enters, or tries to enter, the vehicle while the search is being carried out.

You may use reasonable force (e.g. handcuffing) to effect and continue the detention.

The detention:

- may be for any **reasonable period** but no longer than the duration of the search
- starts when you direct the person to remain and ends when you tell them they are free to go.

(s118)

## Determining a connection

As soon as you have detained a person under section 118, you must take active steps to determine whether there is a connection between them and the search. The detention can only be for the shortest period practicable in the circumstances to determine this.

You cannot simply detain the person for the duration of the search and then on completion, consider the matter of connection. In essence, once people have been excluded and cleared of suspicion, they should be informed that they are free to go about their business.

## Detention for the shortest period practicable

Endeavour to allow occupants back into a place or vehicle as soon as it has been secured and where it is physically practicable (e.g. sufficient room available) for them to be present and where they are not likely to hinder or obstruct the search.

If it is not practicable, you should assist the occupants to find alternative locations such as relatives' or friends' houses to stay while the search is completed.

## Powers to search persons at a place or vehicle

If you are searching a place or vehicle, you may:

search any person...	if you have reasonable grounds to ...
<ul style="list-style-type: none"> <li>- found at the place or in or on the vehicle, <b>or</b></li> <li>- who arrives at the place, <b>or</b></li> <li>- who stops at, or enters, or tries to enter or get into or onto the vehicle</li> </ul>	<ul style="list-style-type: none"> <li>- <b>believe</b> that evidential material that is the object of the search is on that person, <b>or</b></li> <li>- <b>suspect</b> the person is in possession of a dangerous item that poses a threat to safety <b>and you believe</b> that immediate action is needed to address that threat.</li> </ul> <p><b>Exception:</b> An exception to the above is when the search is for drugs - you can then search any person at the scene as a matter of course under section <a href="#">19</a> or <a href="#">21</a>.</p>

(s119)

**Note:** If you **seize** any item posing a threat to safety, then it must, **unless** possession constitutes an offence, be returned to the person:

- once your search has been completed, or
- when you are satisfied there is no longer any threat to safety.

## Powers of search when suspect pursued

If you intend to search a person or vehicle, but that person or vehicle leaves before you are able to start or complete the search:

you may...	if you have...
<ul style="list-style-type: none"> <li>- apprehend the person or</li> <li>- enter any place to apprehend the person or vehicle</li> </ul>	<ul style="list-style-type: none"> <li>- been freshly pursuing the person from the intended search location until apprehended, <b>and</b></li> <li>- you have reasonable grounds to <b>believe</b> that relevant evidential material is still on the person or in or on the vehicle.</li> </ul>

(s120)

**Note:** You can effect the apprehension or undertake the search **only** if you are the officer in fresh pursuit, **unless** you are acting as that officer's assistant under section [113](#) and under their direct supervision and control.

## Risk assessment when planning searches

### Maximising safety and minimising risk

Maximising safety and eliminating or minimising risk when searching is the responsibility of all Police employees and those requested to assist with the search. Safety and risk reduction is met by adherence to police policies designed to manage safety and comply with obligations under the [Health and Safety at Work Act 2015](#). A key enabler is the application of the [TENR-Operational threat assessment](#) in the workplace.

Persons planning and conducting searches must take reasonable care to ensure their acts or omissions do not adversely affect the health and safety of other persons. Searchers must comply as far as practicable with any reasonable instruction given to enhance the safety and well-being of those involved in the search and with the [Health and Safety at Work Act 2015](#) or associated regulations. Investigative considerations are secondary to the safe execution of a search.

### Planning searches of places, vehicles or things

All searches of a place, vehicle or thing by way of warrant or warrantless power must be treated as a critical incident involving risk with the potential to cause harm. Planning must be undertaken to:

- assess any threats arising, manage exposure, determine the necessity to intervene and decide the proportionate response
- identify issues that may impact on community trust and confidence in Police
- problem solve and apply decision-making.

Obtain a search warrant unless it is impracticable to do so (e.g. due to the fluidity and urgency of the situation) and apply contingency management and response arrangements into your operational planning and prepare operation orders.

### Required risk assessments for searches

When planning and executing **any** search you should undertake:

- an [Operational threat assessment \(TENR\)](#)
- a Planned Action Risk Assessment and CARD prompt
- a [critical incident appreciation](#).

### Conducting your risk assessments

When conducting your assessments, follow detailed guidelines in:

- the '[TENR-Operational threat assessment](#)', and '[Community Impact Assessments \(CIAs\)](#)' chapters
- 'Community impact assessment for establishing road blocks', in Search [Part 6 - Roadblocks and stopping vehicles for search purposes](#)
- 'Critical incident appreciation process' in '[Control and command overview](#)'

### Additional risk assessments for search warrants

Before any search warrant is executed, use the [Planned Action Risk Assessment and CARD Prompt](#) to guide your TENR assessment. The CARD prompt then provides a template for the information that must be entered as a CARD event (via iNet-using a mobility device) before the search warrant is executed. (The CARD event should be entered between five and 30 minutes before the search warrant is executed.)

### Urgent situations and re-assessing change

If the situation is urgent, requiring a warrantless search power to be exercised, you may carry out a mental TENR (rather than formal) assessment, and a mental community impact assessment. (The [Planned Action Risk Assessment and CARD Prompt](#) provides a useful aid to assist this). You should also carry out ongoing mental TENR and community impact assessments as the situation changes during execution of the search.

### Planned Action Risk Assessment and CARD Prompt, and 'OnDuty Noting'

Pre-search warrant risk and community impact assessments must be made using the '[Planned Action Risk Assessment and CARD](#)



[Prompt](#) for guidance.

After executing a search warrant, use a mobility device to submit an [OnDuty Noting](#) to provide intelligence information (related to either the subject/s or location) that might be useful to inform future activities.

### **Do not disclose planned action risk assessment without advice**

Do not disclose the planned action risk assessment or [OnDuty Notings](#) without legal advice. A refusal to disclose the assessment can be made under section [16](#)(1)(a) and (c)(iii) of the Criminal Disclosure Act 2008.

## Procedure for planning searches

### Planning for searches

Use this table as a guide when planning searches of places, vehicles and things prior to execution.

Step	Action
1.	Unless circumstances make it impractical, avoid using warrantless powers. Take time to obtain a search warrant.  <b>Note:</b> If a search requires access via adjoining properties, ensure this information is included in the search warrant application.
3.	Undertake thorough risk and community impact assessments applying <a href="#">TENR</a> .  <b>Note:</b> Use the <a href="#">Planned Action Risk Assessment and CARD Prompt</a> to provide a helpful guide to TENR, risk and community impact assessment thinking.  See <a href="#">Examples of risks associated with searches</a> (list is not exhaustive) below.
4.	Undertake a critical incident <a href="#">appreciation</a>
5.	Apply for search warrant using the online Search and Surveillance system, followed by an appearance before an issuing officer.
6.	O/C Search Warrant assesses the <b>response level</b> and <a href="#">assesses the safety options</a> associated with the response level. (Refer to the <a href="#">Planned Action Risk Assessment and CARD Prompt</a> to help guide decision-making).  Response level may include deployment of specialist groups such as: <a href="#">AOS</a> (see steps 7 to 9), <a href="#">Dogs</a> , <a href="#">Clan Lab</a> , <a href="#">SSG</a> , <a href="#">STG</a> .
7.	If AOS is to be involved, have the AOS supervisor check the OC search warrant's risk assessment, safety options and recommended response level. If the risk justifies using AOS, they may need to undertake a reconnaissance to develop: <ul style="list-style-type: none"><li>- a concept of operations</li><li>- detailed pre-deployment briefing.</li></ul> AOS will advise if the operation is beyond their capability.  See the <a href="#">AOS - Pre-planned operation guide</a> to assist with planning if AOS is to be involved and the information the AOS supervisor requires.
8.	The O/C AOS: <ul style="list-style-type: none"><li>- <b>reviews</b> the risk assessments and, if prepared, any concept of operations and pre-deployment briefing document</li><li>- <b>approves</b> any deployment of AOS members (partial or full) and signs off the documents.</li></ul> <b>Note:</b> This includes identification and consideration of principal tactics to be adopted and assets to be used (weapons, breaching, less lethal options, dogs, impact rounds etc.) within the context of identifiable operational limitations.

9.	<p>If AOS is to be used to execute the search warrant, execution is commanded by the AOS O/C.</p> <p><b>Note:</b> The timing and tactical approach is AOS's responsibility. Investigative considerations are secondary to the AOS mission of 'safe execution of the search warrant'.</p>
10.	<p>Execution team conducts pre-execution briefing. The <a href="#">Planned Action Risk Assessment and CARD Prompt</a> provides helpful guidance for final pre-execution risk and community impact assessments.</p>
11.	<p>O/C Search Warrant or a designate enters a CARD event via iNet Viewer between 5-30 minutes before executing the search warrant.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>- This provides essential information for Comms and DCCs to support the safety of executing staff.</li> <li>- The <a href="#">Planned Action Risk Assessment and CARD prompt</a> provides a template for the information required in the CARD event.</li> </ul>

**Note:** These same instructions apply to a warrant to arrest assessed when a search of a place is required to locate the suspect. See the '[Arrest and detention](#)' chapter for further information.

## Examples of risks associated with searches

All searches have inherent risks for employees, those being searched and the community to be factored into planning. Some examples are:

<b>Occupier(s):</b>	<ul style="list-style-type: none"> <li>- May be armed with (or access to) firearms, weapons, explosives, disabling substances</li> <li>- Involved in manufacture or supply of firearms</li> <li>- Have history of violence, disorderly behaviour, resisting arrest, assaults Police, escaping and/or showing signs of aggression</li> <li>- Have aggressive pet(s)</li> <li>- Have history of growing, manufacturing, selling, supplying, consuming or believed to be under the influence of alcohol, drugs and/or psychoactive substances</li> <li>- Are gang members or have association with gangs</li> <li>- Suffering from psychological disorders, depression, suicidal symptoms and medical conditions (e.g. deafness)</li> <li>- Persons being searched may resist.</li> </ul>
<b>Place/vehicle:</b>	<ul style="list-style-type: none"> <li>- Fortified (e.g. gang premises), booby trapped or has security features (e.g. alarms, surveillance cameras)</li> <li>- Occupied by gang members</li> <li>- Dangerous and hazardous substances present or in immediate vicinity (e.g. petrol, chemicals)</li> <li>- Premises with potential hazards (e.g. internal access to adjoining premises, renovations without electrical, plumbing or building consent, open fire operating)</li> <li>- Equipment/machinery present that could be used as a weapon.</li> </ul>

6(c) OIA

<b>Other factors</b>	<ul style="list-style-type: none"> <li>- Children, vulnerable people and public are present or nearby</li> <li>- Supporters of occupier(s) may intervene and be obstructive</li> <li>- Neighbours placed at risk of harm/retaliation.</li> </ul>
----------------------	--

## Safety options to mitigate search risks

Safety options to mitigate risk include:

Option	Description / consideration
Surveillance of the target before execution	Can be with or without a surveillance device. If a device is required, the surveillance regime in the <a href="#">Search and Surveillance Act 2012</a> applies - see the ' <a href="#">Surveillance</a> ' chapter

6(c) OIA

Covert search	Conducting a covert search (approval required from a Detective Senior Sergeant or above - see 'Covert searches' in the ' <a href="#">Search warrants</a> ' chapter)
Entry to other properties	Entry to adjoining or neighbouring properties to the place being searched (see 'Safe execution of warrants - entry to adjoining or neighbouring properties' in ' <a href="#">Search warrants</a> ' chapter)
Risk mitigation strategies	Other options to mitigate risk may include: <ul style="list-style-type: none"> <li>- employees being clearly identifiable as police and Police labelling well displayed</li> <li>- use of uniform patrol vehicles, flashing lights and sirens</li> <li>- path of approach to be taken</li> <li>- having ambulance/medics available near search scene.</li> </ul>

**Note:** See the [Community Impact Assessments \(CIAs\)](#) chapter for generic community impact considerations to mitigate community risks.

## Separating individuals posing risk from premises to be searched

### Tactical arrest or interception in public place

One tactical option available in some circumstances, is separating an extreme risk individual from the premises to be searched. This is commonly referred to as a tactical arrest or interception. This tactical option needs to be lawfully undertaken and if detention or search of any kind is involved, it must be based on a specific power.

If an occupant of the address to be searched is an extreme safety risk (e.g. thought to have access to firearms or other weapons and/or be prepared to use them against Police), consideration must be given to separating that individual from their environment. This may involve:

- surveillance of the individual to ensure absence from the target address
- intercepting (searching/arresting) the individual in a safer location (e.g. public place).

### Planning to separate individuals from premises

Careful consideration is required before separating an individual posing a risk from premises to be searched. Consider these key factors in relation to planning a tactical arrest or interception.

Factors	Description
1	<p>Conduct a comprehensive <a href="#">TENR</a> assessment.</p> <p><b>Note:</b> The overriding principle of TENR is “Safety is Success”. The safety of Police employees, the public, occupiers and suspects must take priority over other matters (even, if necessary, including potential loss of evidence).</p>
2	Contemplate arresting the person before executing the search warrant (if there is sufficient evidence to arrest prior to the search).
3	<p>Consider applying for both a warrant to arrest and for a search warrant if there is sufficient evidence available.</p> <p><b>Note:</b> A warrant to arrest issued in conjunction with a search warrant better enables the interception and arrest in a public place; and at the same time execution of the search warrant.</p>
4	<p>In the absence of grounds to arrest the person, determine:</p> <ul style="list-style-type: none"> <li>- Are there grounds for a warrantless search (particularly if the warrant is for drugs or weapons that could be concealed on the person)?</li> <li>- Does the warrant include the individual’s mode of transportation and power to search his vehicle away from the target address?</li> </ul>
5	Effect a traffic stop or interception away from premises to be searched and obtain individual’s cooperation to voluntarily attend search premises.
6	Consider advice from Legal Advisor on the viability/justification/legality of a tactical arrest or interception type operation.
7	In some circumstances the tactical arrest or interception maybe considered a safer option, but may also potentially introduce significant risk to the public, police or suspect. <a href="#">CIA</a> assessment may be necessary for the tactical arrest or interception phase of the search warrant operation.
8	A tactical arrest or interception should never be considered a default option but rather a tactic for consideration.

## Execution of searches and mandatory notifications to COMMS and DCCs

All searches carry inherent dangers and risks for Police employees and others. Notification must be done in a prescribed 4X CARD event.

### Notification procedures to COMMS and DCCs

#### Warrantless searches

If you are exercising a **warrantless search** on a place, vehicle, or thing you **must** notify COMMS, **unless**:

- impracticable in the circumstances (e.g. out of radio and phone contact);
- your safety or the public's safety, or evidential considerations requires that the search be conducted immediately.

Using your radio (consider who might be scanning the Police radio) or mobile phone advise COMMS:

- your call sign(s), identity and the number of colleagues accompanying you
- event location where search is to be conducted
- time and date search are to commence
- units attending and units carrying firearms
- occupants' details
- contact information for O/C
- target(s) / occupant(s) (PRN / DOB if known)
- of threats, exposure, necessity/authorisation, response/tactics from [TENR](#) mental assessment
- any tactical/additional information relevant to potential escalated response from COMMS.

**Note:** Ensure a 4X CARD event has been notified.

#### Executing search warrants

If you are executing a search warrant:

Step	Action
1	Review the ' <a href="#">Planned Action Risk Assessment and CARD Prompt</a> ' risk assessment. Give special attention to <a href="#">TENR</a> , community impact and staff safety.
2	Ensure all employees are involved in securing a safe environment and those conducting the search are briefed before effecting entry/search
3	<p>Notify COMMS and DCCs of impending search through a 4X CARD event via:</p> <ul style="list-style-type: none"> <li>- INet Viewer</li> <li>- Mobile Responder</li> </ul> <p>The CARD event should contain the following information:</p> <ul style="list-style-type: none"> <li>- 4X -Search Warrant</li> <li>- event location</li> <li>- time and date to be executed</li> <li>- your identity and the number of colleagues accompanying you</li> <li>- units attending</li> <li>- units carrying firearms</li> <li>- target(s)/occupant(s) details (PRN/DOB if known)</li> <li>- contact information for O/C</li> <li>- any <a href="#">TENR</a> (threat, exposure, necessity/authorisation, response/tactics and additional information and also for exercising warrantless search powers when risks have been identified relevant to potential escalated response from COMMS.</li> </ul> <p><b>Note:</b> The 4X CARD event ensures the (mandatory) notification of pending searches authorised by search warrant to both COMMS and DCCs. Remember, this must be carried out between 5-30 minutes before executing the search warrant.</p>

## Covert searches

If you are **executing a covert search** approved by a supervisor (sergeant or above) instead of carrying out the notification procedures for search warrants generally, notify the Shift Commanders at COMMS and DCCs by phone with the confidential details of the pending search covering the points identified for advising [warrantless searches](#).

## COMMS and DCCs responsibilities

Shift commanders at COMMS and shift supervisors at DCCs are responsible for:

- advising only those subordinates on a 'needs to know' basis for safety to monitor the execution of overt search warrants
- keeping sensitive information, particularly involving covert searches, confidential, but still maintain a monitoring role
- responding to and taking command of any emergency that may arise from the execution of the search warrant **-Note:** Comms shift commander will take command of any emergency that may arise from the execution of the search warrant until such time as the District has appropriate resource and people in place to take command of the emergency.
- ensuring risks that are not mitigated are identified and acted upon.

**Note:** Planning, command and control of the execution phase remains with officer in charge executing the search warrant.

## Steps to follow after execution phase

Follow these steps after executing a search warrant:



Step	Action
1	As soon as possible after the warrant is executed, the <b>executing officer</b> (or designate) completes and submits the electronic ' <a href="#">OnDuty Notings</a> ' notification on their mobility device. Note in the Police file that the noting has been done.
2	<b>Learning for the future</b>  Notings should provide information obtained while executing searches that might be relevant to future risk assessments. This will improve our ability to assess risks to the safety of employees executing future responses, and identify measures to reduce the risk of harm to police and others.  If you think there might be a potential risk to other staff conducting search warrants not necessarily connected to your warrant (e.g. through criminals sharing man-trap ideas), notify Comms of the issue so they can pass on emerging trends to other staff in the field and notify <a href="#">Lessons Learnt</a> to ensure the knowledge can be shared.

## Entry, announcement and identification requirements

### Powers of entry

Every search power authorises the person exercising it, to enter and search the place, vehicle or other thing they are authorised to enter and search, and any item(s) found in that place, vehicle or thing, at any reasonable time.

(s [110](#))

### Search warrants to enter and search vehicles

If a search warrant authorises the search and entry of a vehicle, you may enter any place where you have reasonable grounds to believe the vehicle is to locate and search it.

(s [127](#))

### Identification and announcement requirements on entry

If you exercise a search power, you must **before your initial entry**:

- announce your intention to enter and search the place, vehicle, or other thing under a statutory power
- identify yourself (by name or ID)
- if not in Police uniform produce evidence of your identity.

You must also, either **before or on initial entry** provide the occupier of the place or the person in charge of the vehicle or other thing:

- a copy of the search warrant (unless the warrant is issued under section [18D](#) - warrant to search places and vehicles in specified area and seize weapons); **Note:** If it is not possible or practicable to have the search warrant in your possession, you may execute:
  - a facsimile or a printout of an electronically generated copy of the warrant, or
  - a copy which is endorsed to that effect)

See '[Form of written notice when exercising a search power](#)' for information about the strict notice requirements including those for section [18D](#) searches. (s [131](#)(1))

or

- for a warrantless search or securing a scene under section 117 when a warrant is pending, (if requested by any person affected) state the name of the enactment under which you are searching or propose to search and the reason for the search, unless impracticable to do so in the circumstances.

(s [117](#))

**Note:** Where a warrant covers separate units of occupancy, an occupier of each unit searched should be provided with a copy of the warrant. If in doubt, take multiple copies of a warrant to a search scene to distribute if necessary. See [Law Note - Copies of search warrants to be given to all occupiers at properties with multiple dwellings](#)

See [Notice and inventory requirements](#) after search or seizure in this chapter for information about what to do if the occupier or person in charge of the vehicle is not present during the search.

### Exceptions to announcing entry and giving reasons for the search

You do not have to announce your entry, identify yourself and give a copy of the warrant or notice of the reasons for a warrantless search if you have reasonable grounds to believe that:

- no person is lawfully present in, or on the place, vehicle, or other thing to be searched, or
- compliance with the requirements would:
  - endanger the safety of any person, or
  - prejudice the successful exercise of the entry and search power, or
  - prejudice ongoing investigations.

(s [131](#)(2))

## Securing the scene to be searched

If you are carrying out a search, you may, in a manner and for a duration that is reasonable to carry out the search:

- secure the place, vehicle, or other thing searched (scene), or any area within that scene, or any thing found within that scene
- exclude any person from the scene or area, or give them any other reasonable direction, if you have reasonable grounds to believe they will obstruct or hinder you.

If requested by any person affected by the search, you must:

- identify yourself by name or ID
- state the name of the enactment under which the search is taking place and the reason for the search, unless it is impracticable in the circumstances
- if not in Police uniform, produce evidence of your identity.  
(s 116)

## Case Law

Securing the scene to be searched was considered by the Court in [Mahmand v R](#) [2019] NZCA 307. In terms of section 116 powers, what is a reasonable manner and duration to secure a place being searched will depend on all the circumstances. The Court noted that even if their view that the application of section 7 of the Act allowed police officers to invoke the section 116 provisions is wrong, they were satisfied that the common law provides adequate authority for police officers to maintain the security of a property being searched.

Further the Court of Appeal has previously held that the section 117 powers where the application for a search warrant is pending do not preclude authority to take any steps necessary to secure the property and ensure the safety of searchers.

Consideration of section 117 when exercising warrantless powers was given by the Court of Appeal in [Mehrtens v R](#) [2018] NZCA 446. The Court stated that in some situations, it would be appropriate for an officer to use the less intrusive powers of section 117, instead of resorting to a warrantless search. However, the Court held that it was not practicable in this case for the officer to obtain a warrant and exercising the powers of section 117. The powers in section 117 do not extend to securing a person.

[G & B v R](#) [2019] NZCA 32 deals with a collateral purpose and safety concerns/procedures when executing a search warrant on an address linked to gang activity. In this case the Court considered the safety measures taken were genuine and reasonable. The property had connections with a gang and there were multiple connections of the gang to the particular road. In respect of this, the Court stated: "This context justifies the police taking extra steps when carrying out enforcement tasks on a property."

Having a dual purpose for executing a search warrant does not invalidate the search, provided that any actions taken in the pursuit of either purpose do not exceed the scope of the warrant.

## Using force on entry and detaining people at the scene

See [Use of force against persons or property](#) in this chapter.

## Being "in uniform"

Uniform is "distinctive clothing or equipment issued by the Commissioner to be worn by Police employees while on duty and having a colour scheme, pattern or style that enables the person wearing it to be readily identifiable as a Police employee". (s4 Policing Act 2008)

The wearing of BAS as the only uniform item by plain clothed employees conducting searches is not sufficient to meet the criteria for being "in uniform". They must produce identification when exercising search powers.

## Use of force against persons and property

See also [Entry, announcement and identification requirements](#) in this chapter in association with this section.

### Using reasonable force to enter property

When exercising any search power, you (and any assistant under your direction) may use any reasonable force in respect of any property to carry out the search and any lawful seizure.

(s [110](#)(c) and s [113](#)(2)(b))

You may also use reasonable force against any property or person to effect entry where this is justified under section 131(3), e.g. when entry is resisted or refused.

When deciding whether to force entry, you must consider the possibility that such entry may present a danger to:

- the Police party
- the occupants of the premises, including children or other vulnerable people present
- members of the public.

6(c) OIA

## Detaining people at searches of places or vehicles

See [Powers of detention incidental to searches of places and vehicles](#) (s118) in the "Powers incidental to search" section of this chapter.

### Options prior to using force on a person

If a person obstructs or resists you exercising an entry, search, stopping, detention or seizure power, consider these options.

Option	Action
1	Explain that their continued resistance or obstruction is an offence of resisting/obstructing Police against section 23 of the Summary Offences Act 1981.
2	Warn them, if practicable, that they will be arrested for the offence of resisting/obstructing Police if they do not desist immediately.
3	Arrest them for resisting/obstructing Police if: <ul style="list-style-type: none"><li>- impracticable to warn the person, or</li><li>- they continue to resist or obstruct you.</li></ul>
4	For further information, see the <a href="#">Arrest and detention</a> or <a href="#">Use of force</a> chapter.

## What can be searched and seized?

### What can you search?

You can only search for items specified in a search warrant or which are permitted under a warrantless power, and only in places that could contain them. For example, you could not search a drawer for a large television set - although you could for documents relating to it.

A vehicle can be searched if it is on the premises, but a vehicle parked on the street must be specified in the warrant.

### Searching people at the scene

If you are searching a place or vehicle, you may search any person found there, or who arrives at the place or stops at, enters or tries to enter the vehicle, if you have reasonable grounds to believe:

- evidential material that is the object of the search, is on the person, or
- the person is in possession of a dangerous item that poses a threat to safety, and that immediate action is necessary to address that threat.

You can seize any such evidential material or dangerous item from the person.

(s [119](#))

**Note:** In the case of searches for drugs, you may search any person at the scene as a matter of course under section [19](#) or [21](#).

### What can you seize during the search?

Every search power authorises you to seize anything that is the subject of the search or that may lawfully be seized.

(s [110](#)(d))

If you find evidence of an offence other than the one specified in the warrant or covered by your warrantless power, you cannot seize it unless:

- you obtain another warrant, or
- you exercise [plain view](#) seizure under section [123](#).

### Items of uncertain status

If you are not certain if something can lawfully be seized and it is not reasonably practicable to determine that where the search takes place, you may remove the item for examination or analysis to determine whether it may be lawfully seized.

(s [112](#))

This removal power is limited to when you are exercising a search power to find an item but are not sure if the item found is the actual item you are searching for and therefore whether it may lawfully be seized. For example, if you are exercising a search power to locate cocaine and find a package containing white powder, you may remove the package under section 112 for the purpose of examination or analysis to determine whether or not the powder is cocaine and can then lawfully be seized.

The section 112 removal power could not be used, if for example, the purpose of your search is to find cannabis, but you find a television and are uncertain whether it is stolen or not. You would need to consider whether the circumstances are appropriate to exercise a plain view seizure under section [123](#) or to secure the place, vehicle or other thing being searched while an application for a search warrant is pending under section 117. (See 'Special powers when search warrants are pending' in '[Search warrants](#)' for more information).

### Case law

The case [Police v Topia](#) [2018] NZDC 20607 considered sections [112](#) (items of uncertain status) and [123](#) (seizure of items in plain view) with the seizure of a laptop found during a search warrant for other items and examination of an open Facebook account without warrant.

The Court's findings confirmed that items cannot be seized without warrant simply for convenience, where it is practicable to make basic enquiries about them on the spot. Further, the opportunistic searching of a laptop and the contents of a Facebook page

represent a significant intrusion into the owner's privacy- which, if not well-justified, will likely be unreasonable and may result in the exclusion of evidence.

## Seizure of items in plain view

If you are exercising a search power or are lawfully in a place as part of your duties, you may seize any item(s) you find in the course of carrying out the search or as a result of observations at that place, if you have reasonable grounds to believe you could have seized the item(s) under:

- any search warrant obtained under the Search and Surveillance Act or another enactment, or
- any other search power exercisable by you under the Search and Surveillance Act or another enactment.

If you seize an item(s) in circumstances where you are not already exercising a search power, you may exercise any applicable power conferred by s110 in relation to the seizure of the items. (See [Powers incidental to search](#) in this chapter). (s123(3))

## Case Law Roskam v R [2019] NZCA

In [Roskam v R](#) [2019] NZCA items were seized under section 123 of the Act after items subject to the warrant had been seized. In the Court's view it was sufficient that the officers saw the basket containing the electronic equipment and formed a view that its contents may include stolen items and could legitimately be the subject of an application for a second search warrant. Seizure of those items did not overreach into an illicit invasion of privacy, and unlawfully extended search, because the existence of the basket and contents had already been noted. Section 123(2) does not require the police to form an instant view as to criminality. The items were therefore capable of being seized, and fell within the purview of section 123(2).

Section 123 would not have entitled the officers to take a renewed or extended search of the room itself, for example the entering of closed spaces such as wardrobes. The basket and the bags were discrete, portable items. They were capable of being seized, and therefore fell within the scope of section 123(2).

The Court noted that the scene could have been further secured against interference in the meantime under section 117. However, ultimately this second warrant was not needed as the items could be legitimately seized pursuant to section 123.

## Case law: Smith v Police [2019] NZHC 2111

The case [Smith v Police](#) [2019] NZHC 2111 highlights the importance of obtaining a further warrant where evidential material not covered by the warrant authorising entry/search is identified and further searches are required. In particular, s123 (seizure of items in plain view) of the SSA is a seizure power, not a search power. The officers in this case were not able to satisfactorily address/explain the prerequisite in s20(c) that if the "search is not carried out immediately, evidential material relating to the suspected offence will be destroyed, concealed, altered, or damaged."

## Seizing privileged materials

Special rules apply in relation to the search and seizure of privileged or confidential materials held by lawyers, ministers of religion, medical practitioners, or clinical psychologists relating to clients or journalists relating to their sources. See '[Privilege and immunities under the Act](#)'.

## Searching for and seizing computer material

### What computer material can be searched and seized?

The Search and Surveillance Act 2012 explicitly provides for the search and seizure of "intangible data" held in data storage devices such as computers and cell phones. See [Ruru v R](#) [2020] NZCA 64 where a search warrant authorises the search of devices, Police may search communications found on that device (assuming such searches are within scope of the warrant or search power), even if the information at issue was downloaded from an internet server located overseas.

A search of a place, vehicle or thing also extends to the search of any computer system or data storage device located in whole or in part at the place, vehicle or thing.

A search of a business' computer network is therefore permitted even though the server is at premises other than those being searched. A search of any internet data accessible by the computer's user on the premises being searched is also permitted. Thus emails on Gmail or Hotmail or data held in the "Cloud" may be accessible, whether or not the data is downloaded, and whether or not the computer automatically logs on to the internet site when it is switched on. In the event that a password is required, the user may be required to provide the password under section [130](#).

You are not permitted to obtain the password, by way of example, to a Gmail account from the user of the computer that is located in a place being searched and then to conduct a subsequent search of that account from the enforcement agency's computer. That may only be done by way of a [warrant to conduct a remote access search](#).

See [Cloud computing](#) in this chapter for information about cloud computing and how to get information out of "the cloud".

### Intangible material on, or accessible from cell phones or computers

Make sure to identify what intangible material is being sought in warrants for cell phones and computers.

[Tupoumalohi v R](#) [2020] NZCA 117 is an important reminder about specifying in warrants what type of intangible material they are seeking when seizing cell phones or computers. It is insufficient to state that Police wish to seize a particular cell phone. It is necessary to specify in the warrant that intangible material on, or accessible from, the device is also sought. All that was required here was for the search warrant to be issued in terms that expressly allowed the Police to access data, communications and images from the cell phone.

Searching a cell phone after a search warrant has been obtained

When searching a cell phone that has been seized through the lawful and successful execution of a search warrant, it is not necessary to obtain a further warrant for each search that is conducted in accordance with the original search warrant. In order to preserve data, police should adhere to standard practices when seizing cell phones. If a search for other purposes is needed, an additional warrant may be required. See [R v R](#) [2018] NZCA 341 for searching a cell phone after a search warrant has been obtained.

### Definitions related to computers

These meanings of terms relating to computers apply in relation to search powers unless the context otherwise requires.



Term	Definition
<b>Access</b>	Access in relation to any computer system means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system (s3).
<b>Access information</b>	Access information includes codes, passwords, and encryption keys, and any related information that enables access to a computer system or any other data storage device (s3).
<b>Computer system</b>	Computer system: <ul style="list-style-type: none"><li>- means:<ul style="list-style-type: none"><li>- a computer, or</li><li>- 2 or more interconnected computers, or</li><li>- any communication links between computers or to remote terminals or another device, or</li><li>- 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device, and</li></ul></li><li>- includes any part of the items described above and all related input, output, processing, storage, software, or communication facilities, and stored data (s3).</li></ul>
<b>Remote access search</b>	Remote access search means a search of a thing such as an Internet data storage facility that does not have a physical address that a person can enter and search (s3).
<b>User</b>	A user is a person who <ul style="list-style-type: none"><li>- owns, leases, possesses, or controls the system, device, or site, or</li><li>- is entitled, by reason of an account or other arrangement, to access data on an Internet site, or</li><li>- is an employee of one of the above (s130(5)).</li></ul>
<b>Specified person</b>	A specified person is: <ul style="list-style-type: none"><li>- a user of a computer system or other data device or an Internet site who has relevant knowledge of that system, device or site</li><li>- a person who provides an Internet service or maintains an Internet site and who holds access information (s130(5)).</li></ul>

## Search of a computer under warrant

If you are obtaining a warrant and know at the time of application that the search is likely to include the search of a computer, you should:

- be as specific as possible in the application about the material that you are looking for
- where practicable, specify the procedures you will adopt to locate the material (e.g. use keywords to identify relevant files or locate the required material), although it is important to do this in a way that maintains the flexibility to undertake the search effectively.

A warrant that is too general and does not adequately spell out what is being looked for may subsequently be held to be invalid.

## Search of a computer without warrant

If you are searching a computer under a warrantless power, you should:

- conduct the search in a way that most effectively targets the material you are looking for
- distinguish between material that may come within the scope of the search and material which is clearly irrelevant information.

You must not conduct a "fishing expedition" and should avoid appearing to others you are.

## Carrying out a search of a computer

If you are authorised to search a computer (or other data storage device), you may:

- use any reasonable measures to access a computer system or other data storage device located (in whole or in part) at the place, vehicle, or other thing if intangible material that is the subject of the search may be on that computer system or device (s110(h))
- remove the computer for further examination if it is not practicable to search it on the premises (s112)
- take a forensic copy of the hard drive to preserve the evidential integrity of the material (s110(i)) and if you find the material that you are looking for, maintain possession of that data
- require a person who owns, leases, possesses or controls the computer device or system, or an employee of such a person, to provide access information (e.g. password) or other information (e.g. de-encryption information) that is reasonable and necessary to allow you to access the data (s130). (Any person who fails, without reasonable excuse, to assist you exercising the search power when requested to do so, commits an offence (s178)).

## Carrying out a search of a cell phone

The following is general guidance about searching cell phones:

- If a cell phone is seized pursuant to arrest in reliance upon section 88 of the S&S Act or some other without warrant search power, and there is no urgency in respect of its examination, apply for a search warrant to retain and search the cell phone and relevant contents. Urgency may arise where evidential material on the phone or accessible from the phone may be erased or no longer accessible if there is a delay in conducting the search e.g. some applications can be deleted or inactivated remotely. A delay in accessing information may also hinder a Police investigation. The reason for the search and what was searched on the cell phone should be documented.
- When seeking a warrant to seize and search a cell phone, it is necessary to specify in the warrant that intangible material on, or accessible from, the cell phone is also sought (*Tupoumalohi v R* [2020] NZCA 117). If possible, the type of intangible material that needs to be searched should be listed. For example, text messages, emails, communications in applications such as Facebook Messenger or similar types of applications and photographs/videos. Likewise, date ranges could be identified in appropriate cases. Remember, intangible material that is accessible from the cell phone should be captured (synchronised) during the termination of the warrant or execution of the search power.
- Although it may be impossible to anticipate the exact nature and location of data held on a cell phone, it does not follow, however, that it is always impossible to limit the scope of the warrant to data/information/communications of a specified type and/or to named applications or classes of applications, instead of simply authorising the search of a cell phone for a specified purpose (*Ruru v R* [2020] NZCA 64).
- When a cell phone application is lawfully connected to a remote server or the internet, the cell phone becomes part of the computer system. Therefore, if Police are authorised to search the cell phone pursuant to a with or without warrant power, this extends to searching apps if they are within the lawful purpose of the search. A search of internet applications on a seized cell phone does not require a remote access warrant (*Ruru v R* [2020] NZCA 64).

6(c) OIA

- Subject to the parameters of a warrant or search being conducted, any search of a phone should extend only so far as is necessary to investigate the offence for which it was seized. If evidence of other/unexpected offending is identified in plain sight and searches are specifically required for the purpose of investigating that new offending, a new search warrant should be obtained. Section 123 (seizure of items in plain view) of the Search and Surveillance Act may apply, but this section is not a search power. For example, if objectionable publications are identified during a search of a cell phone for drug offending and additional searches of the phone are required to investigate the objectionable publication offending, a new warrant should be obtained.

See [Douglas v Police](#) [2019] NZHC 2672 for case law guidance on cell phone (computer) searches.

6(c) OIA

6(c) OIA

## Remote access searches authorised by warrants

A search warrant may authorise a "remote access search", of a thing such as an internet data storage facility. The issuing officer must be satisfied that the thing is not situated at a physical address that is capable of being entered and searched (s [103](#)(6)).

6(c) OIA

The warrant application should specify why the applicant believes that the data is not held at an accessible location. The warrant must specify with sufficient particularity the access information that identifies the thing to be searched remotely, such as the email address or the logon information relating to the site to be searched.

### Note:

You **can not** obtain a remote access search warrant merely because a server with web-based material is inaccessible in that particular circumstance, e.g. because it is overseas or its location has not been researched. In this event, you should:

- seek the cooperation of the organisation that hosts the server, or
- obtain a production order under s74, or
- seek mutual assistance through the Mutual Assistance in Criminal Matters Act 1992.

## Additional powers when conducting remote access searches

If you are executing a search warrant authorising a remote access search, you may:

- use reasonable measures to access the thing to be searched, and
- copy any intangible material from the thing searched if it is the subject of the search or may otherwise be lawfully seized.

(s [111](#))

**Note:** There are technical and cross border issues that may arise with "remote access searches" and both the Electronic Crime Laboratories and Legal Services must be involved in the preparation of these search warrants. The applications will require careful scrutiny by both groups.

## Principles for data evidence gathering

The general principles of gathering data as evidence are:

Step	Principle description
1	No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
2	Any person accessing original data held on a computer or on storage media must be competent to do so and able to give evidence explaining the relevance and the implications of their actions.
3	An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
4	The person in charge of the investigation (O/C case) has overall responsibility for ensuring that the law and these principles are adhered to.

## Procedures for accessing computers, securing evidence and creating forensic copies

Follow the procedures in [Preservation and recovery of electronic evidence](#) in the 'Crime scenes and forensics' section of the Police Manual when accessing computer systems and making copies of any intangible material found there to ensure the integrity of the evidence is preserved.

See [Cloud computing](#) in this chapter for information about cloud computing and how to get information out of "the cloud".

Note: All remote access search warrant applications and searches must be forwarded to the [ECL](#). Specialist knowledge with remote access searches in this process is required to ensure national and international laws are observed.

### Securing evidence

6(c) OIA

## Disposal of forensic copies

If you make a forensic copy, deal with it as follows:

If the copy...	you...
does not contain any "evidential material" (i.e. material that may be seized)	must ensure that the forensic copy is "deleted, erased or otherwise destroyed in a way that prevents retrieval" ( <a href="#">s161(1)</a> ). In practical terms, this means that you must delete it so that it is not normally accessible on the hard drive.
contains a mixture of evidential material and non-evidential material	may retain the forensic copy in its entirety ( <a href="#">s161(2)</a> ).

## Information tending to incriminate

A specified person may not be required to give any information tending to incriminate themselves. However, this does not prevent you from requiring them to provide information or assistance that is reasonable and necessary to allow you to access data held in, or accessible from, a computer system or other data storage device that contains or may contain information tending to incriminate the person.

## **Privilege and confidentiality**

Powers requiring a person to provide access, information or assistance are subject to the privilege and confidentiality provisions of the Act. (See Part 13 - [Privilege and immunities under the Act](#) for more information).

## Cloud computing

### Information in the cloud

Cloud computing has been around for a long time, but the term is relatively new. Applications, such as Hotmail, Facebook, Gmail and Dropbox are cloud based applications, because they reside in the cloud, i.e. not on your computer.

6(c) OIA

6(c) OIA

## Notice and inventory requirements after search or seizure

### Notice requirements

There are strict notice requirements under sections [131](#) and [132](#) of the Act to be followed by persons exercising a search power or who conduct a remote access search.

### Form of written notice when exercising a search power

The form of notice given before or after a search and seizure varies depending on whether the search was conducted with or without a warrant and whether or not the occupier or person in charge of the vehicle was present during the search.

#### **For you must:**

searches conducted when give that person before or on initial entry:

occupier or person in

charge of vehicle or thing

**is lawfully present**

- copy of the warrant (unless the warrant is issued under section [18D](#) - to search places and vehicles in specified area and seize weapons, see '[Identification and announcement requirements on entry](#)' for further information) and attached privilege information contained in the 'Notice to occupier, or the person in charge of vehicle or other thing present during search', or
- if a warrantless search, a copy of the 'Notice to person present during warrantless search' (POL1275).

#### **Note:**

The exception to this requirement is when you have reasonable grounds to believe an unannounced forced entry is justified in the following circumstances:

- a person is not lawfully present (e.g. a burglar), or
  - compliance would:
    - endanger the safety of any person
    - prejudice the successful exercise of the entry and search power, or
    - prejudice ongoing investigations.
- (s [131](#)(1))



**For you must:**

searches conducted when on completion of the search, leave in a prominent position at the place, or in or on the vehicle or other occupier or person in thing:

charge of vehicle or thing

is **not present**

- a copy of the warrant and attached privilege information contained in the 'Notice to occupier, or the person in charge of vehicle or other thing not present during search', or
  - if a warrantless search, a copy of the 'Notice to person not present during warrantless search' (POL1275).
- (s131(4))

**Note:**

The notice required when occupier or person in charge of vehicle or other thing **is not present** is a written notice containing the following particulars:

- the date and time of the commencement and completion of the search
- the name or unique identifier of the person who had overall responsibility for that search
- if the power is exercised under a warrant issued under section 18D(2) or (3) and a copy of the warrant redacted to show only the particular place or vehicle in respect of which the search power is being exercised is not available at the time of the search, information about how to request a copy of the warrant
- if the power is exercised under a warrant issued under section 18D(4), the name of the enactment under which the search took place and the reason for the search under that enactment
- where the power is exercised without a warrant, the name of the enactment under which the search is taking place and the reason for the search under that enactment
- the address of the office to which inquiries should be made
- if nothing is seized, the fact that nothing was seized
- if anything was seized, the fact that seizure occurred and (if an inventory is not provided at the same time under sections 133 to 135) that an inventory of the things seized will be provided to the occupier of the place or person in charge of the vehicle or other thing no later than 7 days after the seizure.

(s 131(5))

searches resulting in things seized

at the time the thing is seized, or as soon as practicable after the seizure and no later than 7 days after that seizure, provide:

- to the occupier of the place, or the person in charge of the vehicle or other thing, and
- to every other person you have reason to believe is the owner of the thing seized

the following:

- an inventory of items seized (POL 268) and the accompanying 'Notice to owners and others in relation to things seized, **and**
  - a copy of the authority (i.e. a copy of the warrant, POL1275) if the owner is different from the occupier or person in charge and has not previously received the relevant form
- (s 133)

**Note:**

When a search warrant prints off the Search and Surveillance System it will have two attachments, one to be used if the owner is present, the other when they are not. Both attachments have appropriate headings to distinguish them.

## Case Law

Section 131(1)(b) of the Search and Surveillance Act provides mandatory requirements of identification and notice for a warrantless search. *R v Norling* [2018] NZDC 3979 is a reminder to constabulary employees that the notification requirements in section 131(1) of the Act must be complied with. A failure to do so may result in a finding that the search is unlawful.

## Postponing compliance with notice and inventory requirements of items seized

See [Application to postpone compliance](#) for information about when compliance with the requirements to provide written notices about the exercise of a search power and of things seized during the search may be deferred.

## Procedure for recording seized items and providing required notice

Follow these steps if you execute a search warrant or exercise any warrantless search power resulting in the seizure of items.

### StepAction

- 1 Distinguish whether the search is conducted with or without a warrant and whether or not the occupier or person in charge of the vehicle is present or not present during the search. Then follow the appropriate guidelines in the table '[Form of written notice when exercising a search power](#)' above.
- 2 Complete a property record sheet (POL 268), sometimes referred to as an **inventory** of items, in triplicate including:
  - from whom the things were seized and the location
  - a full description of what was seized
  - whether seized under a search warrant or warrantless search power.

Ensure the chain of custody of seized items is properly recorded on the reverse side of the POL 268.

(If no items were seized, this will have been noted on the warrant or the POL1275 in a warrantless search).

- 3 Give the original of the completed POL 268 to the occupier of the place, or person in charge of the vehicle or other thing. The second page of the POL 268 contains the information required under section 133(1) about the authority for the seizure and rights of access to the items and to [claim privilege](#).

If it is not practicable to complete and leave the POL 268 and a copy of the authority for the search at the time of seizure, you must provide them to the occupier of the place or the person in charge of the vehicle or other thing **within 7 days** or seek [postponement](#) under section 134.

**Note:** You **do not** have to provide this information to the occupier of the place or person in charge of the vehicle or other thing from which the seizure took place, if you are satisfied that none of the items seized are owned by that person.  
(s133(2))

- 4 If the owner, occupier of the place, or person in charge of vehicle or other thing is **not present** when things are seized, leave the:
  - completed POL 268 (i.e. the inventory of items seized and notice to owners and others)), **and**
  - the search warrant and appropriate attached notice **or** POL1275 'Notice to person not present during warrantless search'at the address or in the vehicle in a prominent place.

If it is not practicable to complete and leave the documentation, you must provide it to the occupier of the place or the person in charge of the vehicle or other thing **within 7 days** or seek [postponement](#) under section 134.  
(s131(4))

- 5 If you have conducted a remote access search, e.g. of an internet data storage facility, follow the [notice requirements for remote access searches](#) below.
- 6 Retain the duplicate copy of the POL 268 on the file and the triplicate copy remains with the seized property.

## Limits on who can be treated as occupiers or people in charge

No person:

- under 14 years of age (unless found driving a vehicle with no passenger of or over the age of 14 years with authority to consent to the vehicle's search), or
- who you have reasonable grounds to believe is not the occupier of the place or person in charge of the vehicle or other thing.

can be treated as the occupier of the place or the person in charge of a vehicle or other thing for the purposes of section [131](#) and sections [133](#) to [135](#).

(s131(6))

## Notice requirements for remote access search

After completing a remote access search, you must send an electronic message to the email address of the thing searched:

- attaching a copy of the search warrant, and
- setting out:
  - a description of the thing remotely accessed during the search
  - the date and time of the commencement and completion of the search
  - the name and ID of the person who had overall responsibility for the search
  - the address of the office to which inquiries should be made.

If you are unable to deliver the required electronic message (or it is returned undelivered), you must take all reasonable steps to identify the user of the thing searched and to send the required information to them.

(s [132](#))

## Duty to give notice to owners of things that are seized

In addition to providing the occupier of a place or the person in charge of the vehicle or other thing notice of what is seized, section 133(1) requires you to provide to **any person you have reason to believe is the owner of the thing seized**

- written notice specifying what was seized and information about the person's right to have access to the thing or claim privilege in respect of the thing seized, **and**
- a copy of the authority for the search (i.e. the search warrant or for warrantless searches, the name of the enactment under which the search took place).

The section also provides that this information must be provided as soon as practicable after the seizure and, in any case, within 7 days.

You must take care when providing this information to owners following seizure. Search warrants or advice of the exercise of a warrantless power and inventory of items seized (POL 268) all contain details of the location from where the items were seized and except for notices following warrantless searches, the identity of the person from whom they were seized. A POL 268 may also contain details of property belonging to a number of owners. Providing this personal information to the owner(s) of stolen property which is recovered, may pose a threat to the safety of the person from whom it was seized, e.g. the owner of a stolen item may be a gang member wanting retribution.

There are two courses of action available to you if you have concerns about the disclosure of identity information when complying with section [133](#):

**Option Action**

- 1 Delete or mark out the identity and location on the inventory (POL 268) copy and the location of the search on the search warrant copy or the warrantless search power notice copy before providing to the owner.

Seek advice from Legal Services if the owner disputes the deletions from the documents.

- 2 Apply to a Judge for postponement of notice and inventory requirements under section [134](#).

This option has limitations in that the application must be made within 7 days after the warrant is finally executed or the warrantless search power is exercised.

**Notice and inventory requirements relating to production orders**

Use the POL 268 to record items produced pursuant to a production order with appropriate amendments. However, **do not give** the Notice to Owners and Others in Relation to Things Seized on the back of the POL 268 to the person producing the items(s) and others who may have a legal or equitable interest in the item(s). The relevant notice information is contained in the Production order itself and a copy of this must be provided.

**Procedure when seizing items for non-payment of fines**

After seizing items, you must immediately deliver to the defendant, or leave in a conspicuous place on the premises:

- a list identifying the items seized, and
- a notice directing the defendant or the substitute for the defendant to notify the Registrar, within 7 days after the date of the seizure, whether the defendant or the substitute owns or has an interest in the property and to give the Registrar the name and address of any other person who owns or has an interest (including a lease or security interest) in the property.

**Note:** If you use the 'Property Sheet' (POL 268) to list the item(s) seized, then the 'Notice to Owners and Others in Relation to Things Seized' accompanying the form is not appropriate for use in these circumstances. Seek guidance from a Legal adviser with preparing an appropriate notice.

Deliver all seized items to the registrar.

(s99(5)&(6) Summary Proceedings Act)

**Further information**

For further information about seizing property, see also:

- [Accessing and seizing computer material](#) in this chapter
- [Postponing compliance with notice requirements](#) in this chapter
- the [Procedures applying to seized and produced things](#) chapter
- the [Privilege and immunities under the Act](#) chapter.

## Postponing compliance with notice requirements

### Application to postpone compliance with providing notices

If you exercise a search power, you may apply to a judge under section [134](#) for a postponement of the obligation to comply with providing a copy of the search warrant or other authority or a written notice about the search and seizure on the grounds that compliance would:

- endanger the safety of any person, or
- prejudice ongoing investigations.

If the judge is satisfied these conditions exist, they may postpone the obligation to provide a copy of the search warrant, authority or written notice for a specified period not exceeding 12 months.

### Timeframes

An application must be made in the case of:

- a search warrant, at the time of the initial application or until the expiry of 7 days after the warrant is finally executed, or
- any other entry and search power, until the expiry of 7 days after the search power is exercised.

### Application for further postponement or dispensation

If you obtained a postponement order under section [134](#)(3) of the Act, you may, before the expiry of that order, apply to a District Court for a further postponement or dispensation on the grounds that compliance would:

- endanger the safety of any person, or
- prejudice ongoing investigations.

If the judge is satisfied these conditions exist, they may grant a further postponement for a further specified period not exceeding 12 months, or order a permanent dispensation from the obligation to comply.

**Note:** An application for a further postponement may only be made once.

## Restrictions on postponing compliance relating to seized things

A district court judge may not grant any postponement of or dispensation from, an obligation in respect of any thing that has been seized, unless the thing seized is:

- a copy or clone of any information taken or made, or
- possession of a thing by the person from whom it was seized is unlawful under New Zealand law (e.g. a controlled drug found in the possession of a member of the public in circumstances in which possession is an offence against the [Misuse of Drugs Act 1975](#)).  
(s [135](#))

# Search warrants, production orders and examination orders involving media organisations

## Background

From time to time, news media organisations have information about or record the commission of offences on film, tape, photographs or sound recordings while they are covering newsworthy events. Such media material can be important to subsequent Police enquiries or in judicial proceedings and the Police may be duty bound to obtain:

- an examination order for the purpose of seeking information, or
- a search warrant or production order for the purpose of seizing or having produced such film, tape, photographs, sound or digital recordings.

However, news media organisations are very sensitive to the Police having recourse to their information or material for any reason and consider such access to be a potential threat to media freedom. Their principal concern is that reporters, film crews and photographers may be at risk if they are ever perceived by offenders as being gatherers of evidence for Police.

To minimise the risk of complaints when the Police execute search warrants on the premises of media organisations or serve production orders or examination orders, and to ensure compliance with the Search and Surveillance Act 2012 you must follow the procedures below.

## Procedural guidelines (search warrants, production orders and examination orders)

Act **only** where the offence is serious enough to warrant the obtaining of:

- a search warrant, or production order and cannot be otherwise resolved without the seizure of any film, photographs, tape, sound or digital recordings, or
- an examination order and cannot be otherwise resolved without obtaining the information.

Follow these general steps (not necessarily in order) in addition to other requirements detailed in the Search chapter for exercising search, production and examination powers generally.

### Step Action

1 Before you apply for a search warrant or production order obtain the authority of:

- a Police Executive member in the case of Police National Headquarters, or
- a District Commander in the case of a district matter.

If you wish to apply for an examination order you must have the approval of:

- a Deputy Commissioner, or
- an Assistant Commissioner, or
- the District Commander (other than an acting District Commander) of the Police district in which the constable is stationed.

2 Make an application to a Judge unless in the circumstances this is impractical.

3 Maintain close liaison with the "manager" of the particular news media premises prior to the execution of the search warrant, production order or examination order.

Note:

- The exception being where the manager is a suspect or is otherwise involved in the subject matter of the search warrant.
- If the manager is a suspect, seek a search warrant rather than a production order.

The reasons for the execution of a search warrant, production order or examination order should always be explained where it is reasonably practical to do so.

**StepAction**

- 4 Be aware that journalists have rights conferred on them under section 68 of the Evidence Act 2006 to protect certain sources.

If you are serving a production or examination order, or intend to exercise a search power under a search warrant on the manager of a news media outlet and you believe they may be able to claim rights to protect certain sources or other privilege, then you:

- **must** give the manager or their lawyer, a reasonable opportunity to claim a privilege recognised under [Subpart 5 of Part 4](#) of the Search and Surveillance Act 2012, **and**
  - **may**, if you are unable to identify or contact the manager or their lawyer, within a reasonable period:
    - apply to a Judge of the High Court (in relation to journalist's rights to protect certain sources) or to a Judge of the District Court (in respect of all other privileges) for a determination as to the status of the thing, and
    - do any thing necessary to enable the court to make that determination.
- (s145)

- 5 If you receive or expect to receive a claim of privilege and are unable to search a thing pending resolution of the privilege claim, then follow the 'Procedures when searches involve privileged material' (steps 4 to 9) in the chapter "Part 13 - [Privilege and immunities under the Act](#)".

**Note:** You may still secure the thing to be searched, but must not search it, and deliver the thing or copy of it to the court to enable a determination of a privilege claim.

- 6 Where you use any seized material to facilitate interviews of suspects, you should not disclose the source of the material to the persons being interviewed.
- 7 Avoid calling news media personnel, such as reporters, film crews or photographers as witnesses. If this is not practicable, serve a witness summons that describes the seized material being produced in evidence, to preserve the impartiality of the witness.
- 8 In accordance with normal Police practices of evidential disclosure, provide defence counsel with access to seized film, photographs, tape, sound or digital recordings prior to any judicial hearing.
- 9 You should notify an authorised person who represents the particular news media organisation involved of any film, tape, sound or digital recording or photograph that is copied. The notification should include the reasons and the authorisation for doing so, either under the Search and Surveillance Act 2012 or with consent from that authorised person.
- 10 Advise the Manager: Brand and Media at PNHQ as soon as possible where a search warrant is executed on the premises of a media organisation or a production order or examination order is undertaken, so that any media questions directed to the Commissioner can be quickly dealt with.

**Notice to Crown Prosecutor**

The [procedural guidelines](#) must be brought to the notice of the Crown Prosecutor in any case where it is intended to call a member of the news media to give evidence relating to any film, photograph, tape, sound or digital recording seized by Police.

**Protection of journalists' sources**

Note the provision under section 68 and 69 of the Evidence Act 2006. The privilege conferred on journalists under section 68 is recognised for the purposes of the Search and Surveillance Act 2012 (see section 136). See the section '[Procedural guidelines \(search warrants, production orders and examination orders involving media organisations\)](#)' in this chapter.