

Crime Prevention Cameras (CCTV) in Public Places

Table of Contents

Table of Contents	2
Policy statement and principles	3
What	3
Why	3
How	3
Overview	4
Installation and ownership	4
Consultation	4
Operation of CCTV	5
Location	5
Operating times	5
Operational oversight	5
CCTV officer	5
Monitors	5
Control and operation of cameras	6
CCTV information	7
Security and retention of information	7
Public awareness of cameras and collection of information	7
Audits	7
General review	7
Privacy Commissioner	7
Privacy Act 1993 - access and disclosure flow charts	7
Use of information collected	8
Access to information by individual concerned	8
Release/publication of CCTV images	8
Request for access and footage retrieval of digital CCTV data template	9
Appendix A - Example of public notice	10
Appendix B - Checklist/aide memoir	11
Prior to installation and trial of new system or expansion of existing system	11
Consultation	11
Public awareness of crime prevention cameras	12
Camera officer role	12
Control and operation of cameras	12
Security and retention of information	12
Audit, general review and privacy requirements	13
Use of information collected and access to information by individual concerned	13
Appendix C - Evaluation of your CCTV system	15
Factors to consider when evaluating a CCTV system	15
Appendix D – Privacy Act 1993 access and disclosure flow charts	17
Appendix E – Request for access and footage retrieval of digital CCTV data template	19

Policy statement and principles

What

Crime prevention cameras:

- are used to prevent and detect criminal offences in identified high crime areas
- are not used to maintain surveillance on individuals or groups
- must be operated in a manner that complies with the Privacy Act 1993 and this instruction.

Why

The use of crime prevention cameras helps to reduce the incidence of crime and disorder, so that members of the community feel safe when visiting the public areas covered by the cameras.

How

- Police may support local authorities and other groups wanting to install CCTV in public places for crime prevention purposes.
- Use of CCTV may enhance the prevention, detection, investigation, prosecution and punishment of offences.
- Use of CCTV cameras must comply with the Privacy Act 1993
- Police must consult the community prior to the installation of CCTV.
- Where Police monitor CCTV cameras they must maintain operational oversight of the cameras.
- Data collected from CCTV must be destroyed within two months unless required for evidential purposes.
- Sharing of CCTV data is only permissible in accordance with the Privacy Act 1993.

Overview

The objective of installing crime prevention cameras is to reduce the incidence of crime and disorder, so that members of the community feel safe when visiting the public areas covered by the cameras.

This chapter applies to:

- Closed Circuit Television(CCTV) cameras installed at fixed sites in public places for a general crime prevention purpose and operated in conjunction with Police
- crime prevention cameras operated in conjunction with Police but not monitored by Police
- significant expansions of existing crime prevention camera systems
- trials of new systems.

Crime prevention cameras:

- are used to prevent and detect criminal offences in identified high crime areas
- are not used to maintain surveillance on individuals or groups
- must be operated in a manner that complies with the Privacy Act 1993 and this instruction.

Note: Guidelines for operating crime prevention cameras in residential areas are available on the [Neighbourhood Support internet site](#).

Installation and ownership

Consideration must be given as to the information you want to collect, and why do you want to collect it. You should only collect information if you need it.

CCTV cannot be used in a manner that is unlawful, unfair or unreasonably intrusive. Whether collecting personal information by CCTV is unreasonably intrusive will largely depend on the sensitivity of the information being collected, weighed against the seriousness or significance of the reason for collecting it. (For more details refer to the Privacy Commissioner [Guidelines summary](#))

Police may support local authorities and other groups wanting to install CCTV (closed circuit television cameras) in public places for crime prevention purposes.

The camera system will normally be owned by the local authority or other group. They are normally monitored by [Police volunteers](#). However, they may be operated in conjunction with Police and not monitored by Police.

Consultation

Prior to any installation, consult the community to ensure any concerns about the proposal are identified and resolved. Special attention must be given to:

- camera placement (i.e. identified by intelligence)
- appropriate operation of the cameras (including review of recorded material for quality)
- privacy of individuals going about their lawful activities
- establishment of a clear audit and review process.

Operation of CCTV

Location

Collect data so you can see whether CCTV will fix your problem, i.e. collecting statistics on the number and types of crimes in the area, (theft ex-car, assault, fighting, drunkenness, drugs, disorder offences etc.) and the times they occur. This will also help determine whether CCTV has had a positive impact in either deterring criminal activity or assisting in the prosecution of offenders.

Operating times

It is possible for CCTV to record 24 hours, 7 days a week when set to be motion activated without impacting on staffing resources.

Consideration should be given to the hours that CCTV cameras can be monitored in an effort to disrupt or deter criminal activity. Intelligence statistics and local knowledge should be used to assist in identifying crime peaks in an area (e.g. skate parks), and the times or days where these activities peak.

Police should alert local authorities and other interested groups that the cameras will **not** be continuously monitored.

Operational oversight

Where crime prevention cameras are monitored by Police, operational oversight of the cameras must be assigned to a named individual or to a position holder (e.g. shift watchhouse supervisor/station sergeant).

CCTV officer

The Area Commander must designate a CCTV officer to ensure that the installation and operation of the cameras complies with this chapter. Where the cameras are not to be monitored by Police, the Area Commander must designate a CCTV liaison officer who performs an equivalent function and monitors compliance with this chapter and works with [Police volunteers](#).

The CCTV officer is responsible for:

- liaising with the local authority and other interested groups
- alerting the local authority and other interested groups to any deficiencies in the installation and maintenance of the equipment and signs
- confirming the publication of the required public notices (refer [Appendix A](#))
- implementing and updating local operating instructions or policies alongside local authorities
- maintaining the security of the monitors and data storage
- arranging camera training for Police and volunteers
- authorising trained persons to monitor the cameras
- recording relevant statistics and significant incidents, and reporting these where appropriate to the reviewing officer (appointed by Area Commander), local authority and other interested groups
- liaising with the Police Privacy Officer and the Office of the Privacy Commissioner on matters involving Privacy related matters
- assisting in the conduct of a general review of the use of the cameras, and when required, providing specific reports on the need or justification for continued operation of the cameras.

Monitors

Monitors must be installed in either Police premises or some other secure location.

Viewing access to the Police monitors while they are in operation should be restricted to Police employees and persons authorised by the CCTV officer.

Equivalent measures must be taken to ensure the security of monitors that are not operated by Police. Monitors must not be located in such a manner that they can be viewed by the public.

Control and operation of cameras

Operators of the camera equipment are accountable for their actions. The manner in which they use the cameras will be audited and they may be called upon to justify their interest in a particular member of the public (subject to the '[Code of Conduct](#)').

Unless there is sufficient justification for doing so (e.g. reasonable suspicion that an offence is taking place) cameras must not:

- track or zoom in on any member of the public
- be focused on entranceways to buildings or be directed to look through windows into buildings
- view into private residences except as part of a wide angle or long shot or while panning past them.

Note: Only authorised persons have access to camera operation controls.

CCTV information

Security and retention of information

Any information stored on a hard drive must be erased within two months unless it is required for evidential purposes. Any hard drive data required for evidential purposes must be cloned using standard forensic electronic data procedures as used by the Digital Forensic Unit and specified in the [Guidelines for using Digital CCTV Evidence in Law Enforcement](#) as per the Solicitor-General's guidelines.

Access to recorded data must be authorised by the CCTV officer or equivalent and all access to and use of recorded material must be logged.

Public awareness of cameras and collection of information

The Privacy Act 1993 requires that persons from whom personal information is collected are made aware that information is being gathered about them and the purpose for doing so.

The location selected for camera installation must be clearly signposted at the extremities to notify the public that a camera is or may be in operation. The signs also serve as a general crime deterrent.

While the erection and maintenance of signs is the responsibility of the local authority, Police must satisfy themselves of the adequacy of the signs for these purposes.

The signs must clearly display the message **'Police Crime Prevention Camera Area'** or a similar message and be of a size and style that makes them readily visible to people entering the area.

Periodic public notices in the news media (see example in [Appendix A](#)) should convey more detailed information about the purpose and operation of the cameras, including the matters referred to in [Information Privacy Principle 3](#).

Audits

Internal audits must (refer [Appendix B](#)):

- be conducted periodically to ensure compliance with this chapter
- include such matters as the camera operating standards and security of the monitors and data storage devices
- be documented for each audit
- (where appropriate) be conducted jointly with the monitoring agency.

General review

Area commanders must appoint a reviewing officer to conduct a general review of the use of the cameras on an annual basis and to prepare an evaluation report (refer to [Appendix C](#)). Each review must be conducted in consultation with the CCTV officer or equivalent, the local authority and any other group with an ownership or operational interest in any installed camera. The evaluation report should include comment on the location, operation, effectiveness and continuing necessity for the cameras.

Privacy Commissioner

The Privacy Commissioner has the right to review the need for, and the use of the Police crime prevention camera operation in any Police district.

The Office of the Privacy Commissioner must be supplied with this information and any proposal to install new cameras or to expand an existing scheme, at the time of initial consideration. The proposal must include a justification for the installation of the cameras and an outline of the consultation process to be followed. (See the [Privacy Commissioner's Guidelines](#))

Privacy Act 1993 - access and disclosure flow charts

Refer to [Appendix D](#).

Use of information collected

Information collected by the cameras:

- will be used for the deterrence, or immediate detection, of criminal offences which occur in view of the cameras
- may be used, with the prior approval of a Police senior sergeant (or higher rank), for these related purposes:
- inquiries relating to the investigation and prosecution of other criminal offences
- training of Police and persons authorised by the camera officer or equivalent
- research e.g., into the nature of street offences, foot or vehicular traffic systems, or evaluation of the operation of particular camera systems.

Caution: The information must not be used for any other purposes.

Access to information by individual concerned

An individual whose activities have been recorded by a Police crime prevention camera has a right to access and view that personal information provided it is readily retrievable (as it would be in the case of an identified offender). Access can only be refused on one of the grounds set out in sections [27](#), [28](#) and [29](#) of the Privacy Act 1993.

It is good practice to advise suspects early in an interview of the existence of the recorded evidence and their right to access it.

Release/publication of CCTV images

Traditional Police enquiries should be completed prior to publishing CCTV footage of private individuals in the media and social media. This should include internal circulation of images seeking nominations from Police staff. If the individual(s) still remain unidentified, consideration can then be given to external publication taking into account the remaining guidance in this section. Earlier publication can be considered in the event of an immediate risk to public safety.

CCTV footage should only be released if the identity of the individual(s) is unknown; it should not be used to try and verify that the image is that of a nominated suspect.

Under no circumstances should CCTV images of individuals being sought as witnesses, being published.

Police need to be absolutely certain that a crime has been committed by the individual(s) pictured and that there is sufficient evidence to justify the arrest and charge.

Each image should be carefully scrutinised in its entirety and cropping and pixilation should be undertaken as appropriate. The identities of all other individuals within the image; other than the offender should be obscured. Assessment should include the entire image and not just the individuals within the image. For example, does an image taken from inside a shop show anything which could expose security measures and increase the risk of repeat victimisation.

Right to privacy is the first and foremost consideration and therefore publication of images needs to be proportionate to the offence. Give due consideration to the long-term consequences for the individual(s) pictured. The aim is to solve and prevent crime, not to push individuals into reoffending; when they might otherwise respond to alternative interventions. Particular care should be taken not to publish if the individual pictured is clearly an individual whose identity would be protected by law once arrested.

An O/C needs to consider whether a successful prosecution will be reliant on witness identification of the offender, and therefore whether publication of CCTV footage will contaminate witness testimony or remove the opportunity to utilise a montage.

Any decision to publicise CCTV footage in the media or social media should be ratified by a supervisor. Police actions to identify the offender prior to publication should be recorded along with reasons for publication. This provides an audit

trail in the event any complaint is lodged.

Once an individual has been identified media should be updated and the image should be removed from police social media platforms, websites etc. The date and time of this action should be recorded.

Request for access and footage retrieval of digital CCTV data template

Refer to [Appendix E](#).

Appendix A - Example of public notice

 [Example_of_public_notice.doc](#)

33 KB

Appendix B - Checklist/aide memoir

Prior to installation and trial of new system or expansion of existing system

Conditions to be satisfied / work to be completed	Agreed / date completed	Progress / comments
Local authority involved - who is their liaison person?		
Public locations for fixed camera sites - has the justification been documented in terms of crime, place and time?		
Has a crime prevention objective been set for the public areas covered by the cameras?		
Is the use of crime prevention cameras part of a broad crime prevention strategy for the area?		
Have the community been consulted and their concerns about the proposal been identified and resolved?		
Have operation instructions been developed?		
How will the privacy of individuals going about their lawful activities be maintained?		
Have clear audit and review processes been established?		
Is the monitor location secure? Who are the authorised persons who will access the monitors?		
Are local authorities and other interested groups aware the cameras will not be continuously monitored?		
Is there a process for approving and documenting camera use at other times?		
Has operational oversight of the cameras been assigned to a named individual, or to a position holder?		
Has a camera officer been designated?		
Has there been liaison with the Police Privacy Officer?		
Has the Privacy Commissioner been supplied with the proposal, including the justification for the installation of the cameras and an outline of the consultation process to be followed?		

Consultation

Has the district council been consulted?		
Has a public survey been completed?		
Have retailers in the area been consulted?		
Has the public in general been given the opportunity to provide input?		
Has the Police Privacy Officer been consulted?		
Has the Privacy Commissioner been supplied with the proposal?		

Public awareness of crime prevention cameras

Are the locations selected for camera installation clearly signposted and visible to people entering the area?		
Is the local authority aware that the erection and maintenance of signs is their responsibility?		
Do the signs clearly display the message: Police Crime Prevention Camera Area or similar message?		
What is the schedule for inserting public notices in the news media to convey more detailed information about the purpose and operation of the cameras?		

Camera officer role

Liaison with the local authority and other interested groups.		
Alert local authority to deficiencies in the installation and maintenance of the equipment and signs.		
Publish the required public notices in the form appended to the instruction.		
Implement and update the local operating instructions or policies.		
Maintain the security of the monitors and tapes or disks.		
Arrange camera training for Police and volunteers.		
Authorise trained persons to monitor the cameras.		
Record relevant statistics and significant incidents and report these to the reviewing officer, local authority and other interested groups.		
Liaison with the Police Privacy Officer and the Privacy Commissioner.		
Assist the review of the use of the cameras and report on the need or justification for continued operation.		

Control and operation of cameras

Are operators aware they are accountable for their actions?		
Are the cameras being operated in a manner that will stand scrutiny?		
Are only authorised persons operating the camera controls?		
Are operators aware that crime prevention cameras are not used to maintain surveillance on individuals or groups? They are to prevent and detect criminal offences in identified high crime areas.		
Is a logbook being kept recording details of incidents and identifications made attributable to the cameras?		

Security and retention of information

Are tapes being stored securely?		
Are tapes being erased or re-used within two months?		
Are tapes required for evidential purposes being stored according to instructions?		
Is information on hard drives being erased within two months?		
Is hard disk data required for evidential purposes being cloned according to the procedure specified in the Electronic Crime Laboratory instructions?		
Is access to tapes, other media and recorded material being authorised by the camera officer and logged?		

Audit, general review and privacy requirements

What is the schedule for internal audits to ensure compliance with the instruction? Who will conduct it?		
What does the audit include, e.g. camera operating standards, security of the monitors, tapes and drives?		
Has a reviewing officer been appointed to conduct an annual general review and prepare an evaluation report?		
Are the camera officer, local authority and other groups, with an ownership interest, aware of the review process?		
Does the review cover the role of the camera officer?		
Does the review cover the control and operation of cameras and monitors?		
Does the review cover the security and retention of information?		
Does the review cover the location, operation, effectiveness and continuing necessity for the cameras?		
Does the review cover the use of information collected and access to information by individuals concerned?		
Following the installation, was the Privacy Commissioner supplied with an outline of the consultation process followed and copies of the operating policies and public notices issued?		
Has the Privacy Commissioner been sent the latest evaluation report?		

Use of information collected and access to information by individual concerned

Are criminal offences detected or incidents resolved in view of the cameras being documented?	
Has a senior sergeant (or constable with higher rank) approved the use of camera information for inquiries relating to the investigation and prosecution of other criminal offences?	
Has a senior sergeant or (constable with higher rank) approved the use of camera information for training of Police and persons authorised by the camera officer?	
Has a senior sergeant or (constable with higher rank) approved the use of camera information for research into the nature of street offences etc. or evaluation of the camera system?	
Are individuals who request it, and whose activities have been recorded by a Police crime prevention camera, being given access to view that personal information?	
Are suspects being told of the existence of the recorded evidence and their right of access to it early in any interview?	

Appendix C - Evaluation of your CCTV system

Evaluate whether your CCTV system is impacting on the original problem and achieving your original crime prevention and safety outcomes.

Conduct your evaluation by following the steps in this table.

Step	Action
1	<p>Consider:</p> <ul style="list-style-type: none"> • local perceptions of crime and safety • assessing crime statistics, Police intelligence, incident and disclosure data, and other data sources • what other crime prevention measure may have had an impact • the displacement or change in criminal behaviour • whether your technical and procedural audits have contributed to the impact • whether the impacts have been reported publicly. <p>See the 'Factors to consider when evaluating a CCTV system' below this table.</p>
2	Involve your stakeholders and community.
3	<p>Collect information from all available sources like:</p> <ul style="list-style-type: none"> • incident and disclosure books • pre and post-system crime data and statistics • local Police intelligence on crime and policing issues • local media stories • feedback from informal comments or stories of significant change that are discussed in the community • your technical and procedural audits • any other relevant sources.
4	<p>Compare and analyse:</p> <ul style="list-style-type: none"> • What impact (positive or negative) has CCTV had on the problem you sought to solve? • Have you achieved the outcomes in your strategy? • Is the technology and its operation achieving the intended purpose? • How does the CCTV system complement other safety and crime prevention measures? • Whether your systems are capable of determining and resolving problems effectively and lawfully • How and to what degree has crime or criminal behaviour been displaced to other local hot-spots or areas? • What technical advances could improve your system?
5	Publicise your results so that your stakeholders know how effective your system is.
6	Decide whether you are making changes to the CCTV system. Consider removal, upgrade or replacement of your CCTV cameras and systems. Are they effective?

Factors to consider when evaluating a CCTV system

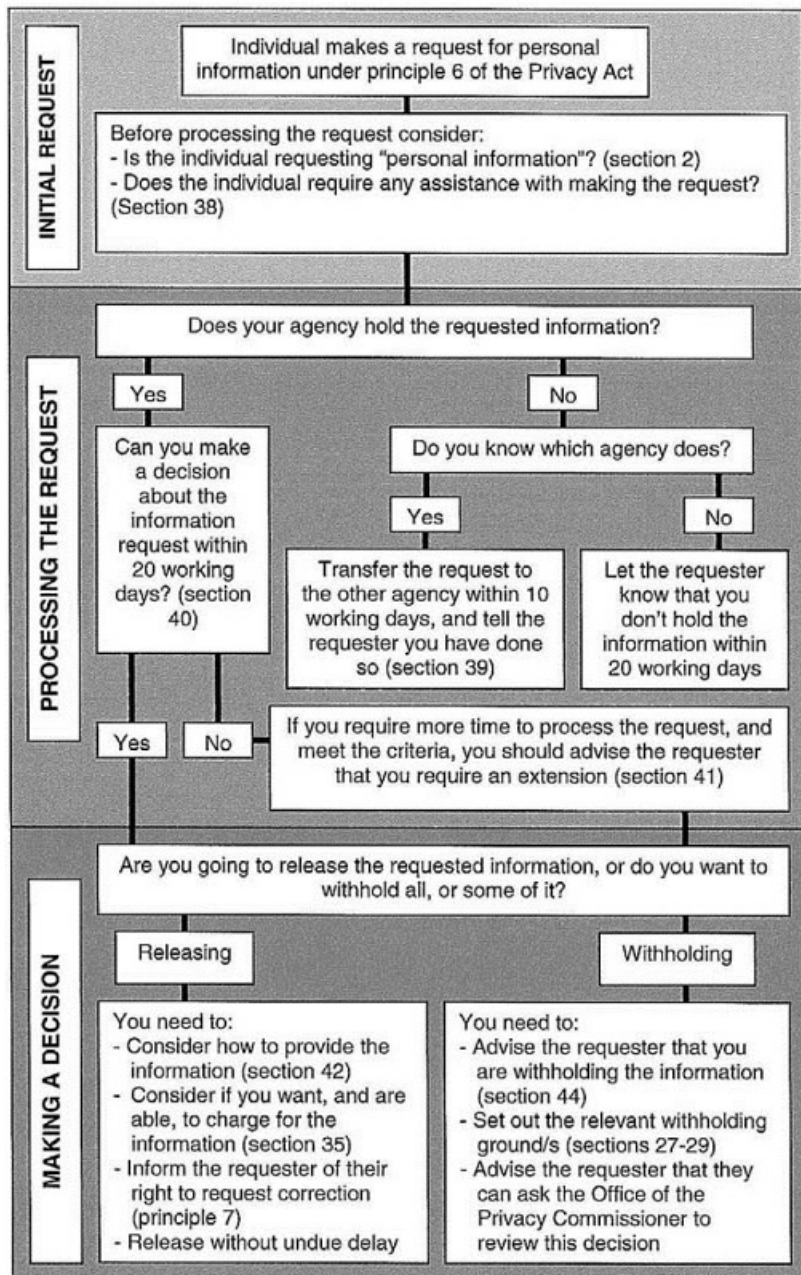
In addition to assessing changes in the levels of crime in the intervention and comparable control areas before and after the installation of CCTV systems, consideration should be given to:

- crime patterns in surrounding areas in order to measure displacement/diffusion of benefit effects
- perceptions among both business traders and the general public of CCTV, fear of crime and feelings of safety in both
- intervention and control areas before and after CCTV installation

- mapping other crime reduction initiatives operating within the intervention and control areas that may impact on any outcomes
- technical specifications and key features of the design of the CCTV systems, such as the number of cameras and coverage area
- the process of implementing and installing the CCTV systems, including any issues that are encountered over the course of the project
- activities aimed at increasing general awareness of the presence of CCTV, such as signage and media releases
- control room operations, including a log of monitoring schedules, details regarding incidents identified by the cameras, calls to Police and/or security patrols in relation to incidents that have been identified, and requests from police for access to footage for evidentiary purposes
- relationships with key external agencies such as Police, including any protocols and procedural guidelines or memoranda of understanding that are developed; and costs attributed to installation, maintenance and monitoring.

Appendix D – Privacy Act 1993 access and disclosure flow charts

DEALING WITH A REQUEST FOR PERSONAL INFORMATION



If you have any concerns on how to proceed with an information request, feel free to contact our enquiries team on 0800 803 909 or enquiries@privacy.org.nz

DISCLOSING PERSONAL INFORMATION (“PI”) UNDER THE PRIVACY ACT (“THE ACT”)

When you have received a request for PI from anyone other than the individual concerned or their representative	Disclosure of PI when you have not received a request
Are you required to release the PI? <i>In some cases you may not have a choice about providing requested information, eg if Police produce a search warrant or if the request is under s 17 of the Tax Administration Act.</i>	Are you required to release the PI under another piece of law? <i>Some laws place agencies under an obligation to report certain information, eg s 18 of the Land Transport Act 1998</i>
<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
Where another law specifically requires disclosure, this overrides the Act. You can disclose the PI.*	Where law specifically requires disclosure, this overrides the Act. You can disclose the PI.*
Are you allowed to release the PI under another law? <i>In some cases you have the discretion to disclose information, but only if you have received a request first, eg the Official Information Act 1982 or s 59 of the Housing Restructuring and Tenancy Matters Act 1992 (HNZC).</i>	Is there another law which allows you to disclose this information? <i>Some laws permit disclosure in specific circumstances or for specific reasons, eg ss 15-16 of the Children, Young Persons and Their Families Act 1989 or the Protected Disclosures Act 2000.</i>
<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
If you want to disclose this information, you may do so.*	If you want to disclose this information, you may do so.*
You will need to consider disclosure under principle 11 of the Act.	
Does an exception under principle 11 apply in the circumstances? Some exceptions allowing for disclosure under rule 11: <ul style="list-style-type: none"> - Where disclosure is one of the purposes which you collected the information for, or disclosure is directly related (principle 11(a)). - If the individual consents to disclosure (principle 11(d)). - If the information was originally obtained from a publicly available publication (principle 11(b)). - Disclosure is necessary to avoid prejudice to the maintenance of the law, or for court or tribunal proceedings (principle 11(e)). - Disclosure is necessary to prevent or lessen a serious threat (having regard to likelihood, severity and imminence) (principle 11(f)). 	
<input type="checkbox"/> Yes <input type="checkbox"/> No	
You can disclose the information, if you want to.*	Do not disclose the information.
*You should also make a note of what PI was disclosed and your reasons for disclosure.	

If you have any questions or concerns about disclosing personal information, feel free to contact our enquiries team on 0800 803 909 or enquiries@privacy.org.nz for guidance.

Appendix E – Request for access and footage retrieval of digital CCTV data template

 [REQUEST FOR ACCESS AND FOOTAGE RETRIEVAL.doc](#)

62 KB

CCTV chapter appendix E