YOUR LIBRARY

Closed-Circuit Television (CCTV) Policy

Approval: Board

Endorsement Date: 29/8/2024

Current Version: 2

Review Cycle: 3 years unless the Board deems an earlier review is required.

Review Date: Every 3 years and no later than 31 December in the review year.

It is recognised that, from time to time, circumstances may change leading to the need for minor administrative changes to this document. Where an update does not materially alter this document, such a change may be made administratively and noted in document history.

Document History

Date	Change Type	Version	Review Year
24/08/2017	-	1	-
29/08/2024	Review and format update	2	2027

Contents

1. Preamble

Your Library Limited uses Closed-Circuit Television (CCTV) to address public safety issues and to assist Your Library meet its legal requirements: under legislation such as the Child Wellbeing and Safety Act 2005, the Child Safe Standards effective from 1 July 2022; and for crime prevention and detection; protection of customers; and to provide a safer physical environment for members of the public.

Considering the purpose and potential use of CCTV data and footage, it is important for Your Library to have a policy to regulate the management of its CCTV systems.

The Closed-Circuit Television Policy (the Policy) has been developed to regulate the management of CCTV in all premises under the control of the Your Library Limited.

The Policy regulates the use of CCTV including collection; retention; security; privacy; access; disclosure; storage; disposal; monitoring and evaluation.

CCTV footage gathered by Your Library will be:

- collected and used for a legitimate purpose.
- related to the activities of Your Library.
- proportionate to its legitimate purpose.

Your Library uses the Guiding Principles and Checklist of the Office of the Victorian Information Commissioner (OVIC) to identify and evaluate its surveillance practices and take a privacy and human rights enhancing approach to its use. Refer to Attachment 1.

2. Background

Your Library is currently using CCTV on a limited basis, either directly or in partnership with its Member Councils. Your Library, and its Member Councils, use CCTV for the purposes of: crime prevention and detection; protection of customers; and to provide a safer physical environment for members of the public.

While CCTV usage by Your Library is limited at present, it is anticipated that over the next 12 to 18 months that either Your Library, either solely or in partnership with its Member Councils, will introduce, or improve, this technology in all our branches.

3. Definitions

Closed-circuit Television (CCTV)	A surveillance system in which a number of cameras are connected through a closed-circuit. The footage taken by the cameras is sent to a television monitor or recorder. CCTV systems consist of cameras, monitors, recorders, interconnecting hardware and support infrastructure.
CCTV footage	Any information that is recorded or unrecorded that is taken from a surveillance system including any data, still images or moving images.
Disclosure	Access to and disclosure of CCTV footage and records to third parties.
FOI	Freedom of Information (in reference to the Freedom of Information Act 1982 (Vic))
IPP	Information Privacy Principles

Live View	An optional CCTV system feature which allows a real-time view of selected public areas to be displayed on a screen accessible to library employees for the purposes of monitoring or security.
Member Councils	Knox City Council, Maroondah city Council, Yarra Ranges Council
Passive monitoring	Where CCTV monitors are intermittently viewed by operators.
Public place	Any place to which the public has access as of right or by invitation, whether express or implied and whether or not a charge is made for admission to the place.
Retrospective review	Where CCTV footage is reviewed after an incident.

4. Privacy of members of the public and its employees.

Your Library will balance the need for passive surveillance against the right for privacy of members of the public and its employees. Your Library will endeavour to ensure that the limitation of any human rights or civil liberties of individual members of the public or employees is reasonable, justified, proportionate, rational and balanced.

In specific relation to privacy requirements, Your Library will endeavour to adhere to all Commonwealth and State legislation and any applicable enforceable guideline covering the operation or use of a CCTV system.

With the exception of matters under investigation by Commonwealth and State law enforcement agencies, footage generally will only be accessed (viz. retrospective monitoring) where: there is an incident and an Incident Report is completed; a child abuse allegation, concern or complaint is raised; or a customer complaint is received.

Your Library reserves the right, where required on a temporary basis, to use its CCTV for live viewing with the aim of improving the immediate safety and security of library users and employees.

Where the CCTV system is owned and operated by a Member Council, Your Library will be bound by that council's policies and guidelines.

5. CCTV Surveillance Systems

Any decision to implement a new, or retain/improve an existing, CCTV system will be made by the Chief Executive based on an assessment of the need for such implementation and the proposed use of the system consistent with this Policy and the relevant privacy legislation.

The CCTV system will have a minimum built in storage capacity to capture footage (24/7) for up to 14 days. At that point, the hard disc will be automatically wiped clean, and recording will recommence. Only footage downloaded for reasons in accordance with Access to CCTV Footage will be retained.

6. Responsibilities and accountabilities

CCTV Register

Your Library will maintain of a register of its CCTV installations, their operational hours, and authorised employees and contractors.

Authorised Access

Access to CCTV footage is limited to authorised employees or contractors with a legitimate reason to access the footage or the equipment.

Authorised Employees include Branch Managers and Team Leaders and designated head-office employees.

All Authorised Employees will undertake training on privacy and understand the contents of this Policy, including the legislative requirements to ensure that the requirements of privacy are understood.

Shared Locations

In instances where certain library branches are co-located with other services within Member Council facilities, the CCTV system may be shared across the entire location. In such cases, where the CCTV system is managed by the Member Council, the Council's CCTV policies will govern its operation and usage.

7. Recorded Imagery/Footage

Access to CCTV Footage

Recorded footage captured may be made available to/in the following parties or situations:

Externally

- An authorised Police member in relation to an offence or suspected offence on receipt of a request in writing.
- An external enforcement agency where an exemption under privacy legislation applies on receipt of a request in writing.
- A Court Order via Subpoena.
- Where otherwise required by law, such as a Freedom of Information (FOI) request.

Internally

- To an Authorised Employee, where the footage is required in relation to:
  - an incident, or potential incident, that is the subject of an Incident Report.
  - criminal behaviour, vandalism, and other anti-social behaviour.
  - child or any other kind of abuse.
  - complaints involving library users and/or other library users or employees.

Retention, storage and destruction of recorded footage

Whilst records should not be destroyed while there is still a need for them, it is also important not to keep records longer than necessary. This will minimise storage costs and administrative overheads, comply with privacy requirements and reduce the risk associated with inappropriate information release.

The CCTV system will have storage capacity to capture footage (24/7) for up to 14 days. At that point, the recordings will be automatically wiped and recording will recommence.

Only footage downloaded for reasons in accordance with Principle 3 will be retained.

CCTV footage relating to the operation of the CCTV systems are outlined in PROS 07/01 VAR 7 Retention and Disposal Authority for Records of Common Administrative Functions. In most cases, surveillance camera footage is temporary and may be destroyed when administrative use has concluded. Accordingly, in such instance's agencies can legally erase the CCTV footage from digital media once the minimum period has expired.

Your Library has decided that the maximum period will be 14 days to protect the privacy of members of the public and its employees.

However, when footage is used to investigate and document specific or significant incidents, Your Library may need to retain the footage for longer periods. For example, records relating to a serious injury of an employee or member of the public are considered permanent and will not be destroyed until legal advice to the contrary is received.

Where footage has been provided to a third party (e.g. Victoria Police, WorkSafe), it is the third party's responsibility to retain the record of the footage in accordance with the Disposal Authority that covers their agency's functional responsibilities. Once Your Library has confirmation that the third party has a working copy of the footage, Your Library will delete its copy of the footage.

The hard drives of the CCTV system will be degaussed and reformatted when they are decommissioned. When hard drives containing sensitive information are decommissioned, they will be wiped permanently using industry best practice.

8. Security and Maintenance of CCTV equipment

Security Measures

Appropriate security measures will be taken to protect against unauthorised viewing, access to, alteration, disclosure, accidental loss or destruction of recorded material.

This security may incorporate physical, administrative or electronic measures, for example, equipment racks, authorisation procedures, electronic passwords, encryption.

Location of CCTV Equipment

CCTV screens and recording devices will not be located in a public area. Where practicable equipment will be located in a secured equipment rack or employees' workroom.

Maintenance

Recording equipment will be checked on a regular basis to ensure the equipment is in good working order.

9. Other Related Matters

Breaches of this Policy

Where an employee is in breach of this Policy, there will be an internal review in accordance with the Employee Performance and Conduct in the Workplace Policy.

Legislation

CCTV surveillance systems are to be operated and managed in accordance with all relevant Commonwealth and State legislation. The list below is not complete and is a guide only because legislation continually changes and new legislation is continually being applied.

Surveillance Devices Act 2004 (Comm)

Privacy Act 1988 (Comm)

Freedom of Information Act 1982 (Comm)

Privacy & Data Retention Act 2014 (Victoria)

Public Records Act 1973 (Victoria)

Private Security Act 2004 (Victoria)

Charter of Human Rights and Responsibilities Act 2006 (Vic)

Freedom of Information Act 1982 (Victoria)

Evidence Act 2008 (Victoria)

10. Other Relevant Your Library Policies & Guidelines

- Membership, Access & Use Policy
- Code of Conduct – Library Users
- Information Privacy Policy
- Information Collection Statement
- Extended Hours Access Policy
- Child Safe Policy
- Child Safe Code of Conduct
- Child Safe Standards
- Child Safe Reportable Conduct Scheme Procedures

11. Disclaimer

Your Library strives to provide information as accurately as possible. The information provided in this Policy is intended as general information only.

Your Library makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the contents of this Policy, and expressly disclaims liability for errors and omissions in the contents of this Policy.

12. Queries about the CCTV System

Your Library will respond to queries in relation to the operation of its CCTV systems. Queries in relation to any aspect of the CCTV system must be made in writing to:

Your Library Limited
10 Caribbean Drive
Scoresby VIC 3179

or by email to:
support@yourlibrary.vic.gov.au

Any member of the public that is dissatisfied with the outcome of their query to Your Library can contact the Victorian Information Commissioner as follows:

Post
Office of the Victorian Information Commissioner
PO Box 24274
Melbourne VIC 3001

Phone
Call 1300 006 842 (1300 00 OVIC) between 9am and 5pm, Monday to Friday.
International callers may call +61 3 8684 7565

Email
enquiries@ovic.vic.gov.au

Appendix 1

Office of the Victorian Information Commissioner (OVIC) - principles for surveillance and guidance principles for surveillance checklist

Principles

Your Library's CCTV systems will be operated in accordance with the OVIC principles for surveillance. In addition, this policy has been assessed against the OVIC guidance principles for surveillance checklist.

PRINCIPLE 1: LEGALITY

Your Library:

1.1 ensures all surveillance is lawful.

1.2 will undertake a privacy impact assessment when next reviewing this Policy.

1.3 complies with the Information Privacy Principles when collecting personal information and sensitive information through surveillance.

1.4 periodically reviews its surveillance practices to ensure they remain lawful.

OVIC legality checklist

Question	Response	*Guiding Principle*
Is the surveillance lawful?	Yes. Your Library has used its best endeavours to ensure that this Policy meets its obligations under any applicable legal restrictions in enabling legislation and other state and Commonwealth legislation has been considered. This includes consideration of the Information Privacy Principles in the Privacy and Data Protection Act 2014 and the Charter of Human Rights and Responsibilities Act 2006. Your Library's CCTV system will be used to: • deter/capture criminal behaviour, vandalism, and other anti-social behaviour. • monitor pubic areas to deter/capture child (or any other kind of) abuse. • assist in the protection of library users. • provide a level of security for employees with face to face public contact. • resolve issues and complaints involving library users and/or other library users or employees. • provide enhanced security of assets, including library materials and equipment.	**1.1, 1.3**

Question	Response	*Guiding Principle*
Has a privacy impact assessment been undertaken?	No. It is intended, although not a statutory requirement, to undertake a privacy impact assessment with the next review of this Policy. *OVIC: Privacy Impact Assessment Guide and Template.*	**1.2**
Is there a plan to periodically review the surveillance after implementation?	Copies of this Policy and the Information Privacy Policy are available in the library branches or on the Your Library website. The Policy will be reviewed every two years, or updated if the legalisation is amended or changed in the interim. The CEO or their delegate is responsible for this Policy.	**1.4**

➢ PRINCIPLE 2: LEGITIMATE AIM

Your Library

2.1 only collects personal information by surveillance when that surveillance is connected to a legitimate aim that directly corresponds to the organisation's functions or activities.

2.2 limits the use of personal information collected through surveillance to the primary purpose for the surveillance or a permitted secondary purpose.

OVIC legitimate aim checklist

Question	Response	*Guiding Principle*
How does the surveillance connect or relate to the organisation's functions or activities?	Because libraries are public spaces where membership is not required and while individuals could be approached for information they do not have to cooperate and may escalate the situation endangering either staff or the general public. Situations include: ➢ deter/capture criminal behaviour, vandalism, and other anti-social behaviour. ➢ monitor pubic areas to deter/capture child (or any other kind of) abuse. ➢ assist in the protection of library users. ➢ provide a level of security for employees with face to face public contact. ➢ resolve issues and complaints involving library users and/or other library users or employees. ➢ provide enhanced security of assets, including library materials and equipment.	**2.1**

Question	Response	*Guiding Principle*
How will the organisation ensure personal information collected through surveillance is only used for the purpose for which it was collected?	Recorded footage captured may only be made available by the ***Authorised Officer*** to/in the following parties or situations where a written/electronic request is received: ***Externally*** • An authorised Police member in relation to an offence or suspected offence on receipt of a request. • An external enforcement agency where an exemption under privacy legislation applies on receipt of a request in writing. • A Court Order via Subpoena. • Where otherwise required by law, such as a Freedom of Information (FOI) request. ***Internally*** • to an Authorised Employee, where the footage is required in relation to: ➢ an incident, or potential incident, that is the subject of an Incident Report. ➢ criminal behaviour, vandalism, and other anti-social behaviour. ➢ child or any other kind of abuse. ➢ complaints involving library users and/or other library users or employees. The Authorised Officer is the Chief Executive or their delegate. There may be situations where the response by Police (e.g. sexual abuse or physical assault) and Emergency Services (terrorist attack) will be time critical. In these situations, a request in writing will not be practicable. The Branch Manager or Team Leader is authorised to make the footage available once they have satisfied themselves as to the identity of the officer making the request. The Branch Manager or Team Leader will advise the Authorised Officer of their action as soon as practicable.	**2.2**

➢ PRINCIPLE 3: NECESSITY

Your Library

3.1 limits personal information collected through surveillance to that which is demonstrably necessary to achieve a legitimate and lawful aim.

3.2 does not use surveillance to collect personal information about an individual, where it is reasonable and practicable to collect the personal information directly from that individual without using surveillance.

OVIC necessity checklist

Question	Response	*Guiding Principle*
Why is the surveillance necessary to achieve the legitimate and lawful aim identified?	Surveillance is required for legitimate and lawful aims, where the individual cannot otherwise be identified, including: ➢ an incident, or potential incident, that is the subject of an internal Incident Report, or escalated to the Police or another external enforcement agency where an exemption under privacy legislation applies ➢ criminal behaviour, vandalism, and other anti-social behaviour. ➢ child, elderly, racial or any other kind of abuse. ➢ complaints involving library users and/or other library users or employees	**3.1**
Is it reasonable and practicable to collect the information directly from the individual, instead of using surveillance?	Because libraries are public spaces where membership is not required and while individuals could be approached for information they do not have to cooperate, and interaction may escalate the situation endangering either staff or the general public.	**3.2**

➢ PRINCIPLE 4: PROPORTIONALITY

Your Library

4.1 assesses the proportionality of the surveillance required in the particular circumstances of an individual case, to ensure the surveillance is carried out in a way that is least likely to impact on privacy and human rights.

4.2 limits surveillance to the least intrusive acts, practices, or methods that are necessary to achieve a legitimate and lawful aim.

4.3 limits surveillance to relevant individuals only.

OVIC proportionality checklist

Question	Response	*Guiding Principle*
Has the proportionality of the surveillance required in the particular circumstances been considered?	Because libraries are public spaces where membership is not required and while individuals could be approached for information they do not have to cooperate and may escalate the situation endangering either staff or the general public. The CCTV system will have storage capacity to capture footage (24/7) for up to 14 days. At that point, the hard disc will be automatically wiped clean and recording will recommence. Only footage downloaded for reasons in accordance with Principle 3 will be retained.	**4.1, 4.2, 4.3**

➢ PRINCIPLE 5: SAFEGUARDS

5.1 Your Library implements procedural safeguards when using surveillance and ensures these safeguards are effective and adequately resourced.

Transparency

Notifications

5.2 Your Library at or before the time (or, if that is not practicable, as soon as practicable after) it uses surveillance to collect personal information about an individual, takes reasonable steps to ensure that the individual is aware of:

a) the identity of the organisation using surveillance and how to contact it; and

b) the fact that the individual can gain access to the information collected through surveillance; and

c) the purposes for which the surveillance is being used; and

d) to whom the organisation usually discloses information collected through surveillance; and

e) any law that enables the surveillance to be used.

Openness

Your Library:

5.3 makes available a document setting out the sorts of personal information it collects through surveillance, its purposes for using surveillance, the specific surveillance practices it uses for collection, and how collected personal information is used and disclosed.

5.4 considers proactively publishing policies and records in relation to its use of surveillance.

Access to personal information

5.5 Your Library provides individuals whose personal information has been collected through surveillance with the ability to request access to that information.

De-identification

Your Library:

5.6 takes reasonable steps to destroy or permanently de-identify personal information collected through surveillance if it is no longer needed.

5.7 considers the risks of re-identification when de-identifying personal information, and destroys personal information collected through surveillance where the risk of re-identification cannot be reduced to very low.

Anonymity

5.8 Your Library only collects anonymous information through surveillance, rather than personal information, wherever it is reasonably practicable.

Information sharing

Your Library:

5.9 limits the sharing and disclosure of personal information collected though surveillance to the primary purpose of the surveillance or a permitted secondary purpose.

5.10 does not transfer personal information collected about an individual through surveillance to someone (other than the collecting organisation or the individual) who is outside of Victoria, unless permitted by the IPPs.

Information security

5.11 Your Library takes reasonable steps to protect personal information collected through surveillance from being misused, lost, or accessed, modified, or disclosed by unauthorised persons.

OVIC privacy safeguards checklist

Question	Response	*Guiding Principle*
What steps are taken to provide individuals with notice of the surveillance?	CCTV signage will be: • Displayed prominently at each main access to the premises. • Designed to be easily understood by members of the public. • Be clearly visible, distinctive and located in areas with good lighting, placed within normal eye range and large enough so that any text can be read easily. • Provide contact details for any queries about the CCTV system.	**5.2**
Are policies and records in relation to the surveillance use published, including the purposes of surveillance and how collected personal information is used?	Copies of this Policy and the Information Privacy Policy are available in the library branches or on the Your Library website	**5.3, 5.4**
Are individuals able to make a request for access to personal information collected through surveillance?	Yes.	**5.5**

Question	Response	*Guiding Principle*
Does a process exist to either de-identify or destroy personal information collected through surveillance when it is no longer required?	Yes. Whilst records should not be destroyed while there is still a need for them, it is also important not to keep records longer than necessary. This will minimise storage costs and administrative overheads, comply with privacy requirements and reduce the risk associated with inappropriate information release. The CCTV system will have storage capacity to capture footage (24/7) for up to 14 days. At that point, the hard disc will be automatically wiped clean and recording will recommence. Only footage downloaded for reasons in accordance with Principle 3 will be retained. CCTV footage relating to the operation of the CCTV systems are outlined in PROS 07/01 VAR 7 Retention and Disposal Authority for Records of Common Administrative Functions. In most cases, surveillance camera footage is temporary and may be destroyed when administrative use has concluded. Accordingly, in such instance's agencies can legally erase the CCTV footage from digital media once the minimum period has expired. Your Library has decided that the maximum period will be 14 days to protect the privacy of members of the public and its employees. However, when footage is used to investigate and document specific or significant incidents, Your Library may need to retain the footage for longer periods. For example, records relating to a serious injury of an employee or member of the public are considered permanent and will not be destroyed until legal advice to the contrary is received. Where footage has been provided to a third party (e.g. Victoria Police, WorkSafe), it is the third party's responsibility to retain the record of the footage in accordance with the Disposal Authority that covers their agency's functional responsibilities. Once Your Library has confirmation that the third party has a working copy of the footage, Your Library will delete its copy of the footage. The hard drives of the CCTV system will be degaussed and reformatted when they are decommissioned. When hard drives containing sensitive information are decommissioned, they will be wiped permanently using industry best practice.	**5.6**

Question	Response	*Guiding Principle*
If the personal information is being de-identified, has the risk of re-identification been assessed?	Yes. The hard disc will be automatically wiped clean and recording will recommence. The hard drives of the CCTV system will be degaussed and reformatted when they are decommissioned.	**5.7**
Is information collected through surveillance anonymous (rather than personal information) wherever reasonably practicable?	Yes	**5.8**
Is any information sharing limited to the purpose for the surveillance being undertaken?	Recorded footage captured may only be made available by the ***Authorised Officer*** to/in the following parties or situations: ***Externally*** • An authorised Police member in relation to an offence or suspected offence on receipt of a request. • An external enforcement agency where an exemption under privacy legislation applies on receipt of a request in writing. • A Court Order via Subpoena. • Where otherwise required by law, such as a Freedom of Information (FOI) request. ***Internally*** • to an Authorised Employee, where the footage is required in relation to: ➢ an incident, or potential incident, that is the subject of an Incident Report. ➢ criminal behaviour, vandalism, and other anti-social behaviour. ➢ child or any other kind of abuse. ➢ complaints involving library users and/or other library users or employees. The Authorised Officer is the Chief Executive or their delegate.	**5.9**
Is personal information collected through surveillance stored in Victoria or a jurisdiction with equivalent privacy protections?	Stored only in Victoria	**5.10**
What steps are taken to protect personal information collected through surveillance from being misused, lost, or accessed, modified, or disclosed by unauthorised persons?	Limited access and authorisation processes.	**5.11**
What resourcing has been allocated to ensure all safeguards are considered and effective?	Manager Business Systems is responsible for maintenance and control of Your Library CCTV systems.	**5.1**

➢ PRINCIPLE 6: NON-DISCRIMINATION

6.1 Your Library does not use surveillance in a manner that discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

OVIC non-discrimination checklist

Question	Response	*Guiding Principle*
Is the surveillance non-discriminatory with respect to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status?	Every Victorian has the right to equal and effective protection against discrimination, and to enjoy their human rights without discrimination. Your Library observes its responsibilities in relation Victoria's Charter of Human Rights and Responsibilities contains 20 basic rights that promote and protect the values of freedom, respect, equality, and dignity. Your Library always considers Charter rights, including the right to equality, when they develop policies and deliver their services.	**6.1**

➢ PRINCIPLE 7: COMPLAINTS AND REMEDY

Your Library:

7.1 provides information and pathways for individuals to complain directly to the organisation where they believe their privacy has been interfered with.

7.2 works constructively to remedy privacy complaints involving surveillance where they are escalated to the Information Commissioner.

OVIC complaints and remedy checklist

Question	Response	*Guiding Principle*
What processes exist to ensure individuals are aware they can complain to the organisation and/or the Information Commissioner where they believe their privacy has been interfered with?	This policy and our information Privacy Policy details the avenues of complaint available to the individual, including contact information for the Information Commissioner.	**7.1, 7.2**