

MONASH CITY COUNCIL CCTV SURVEILLANCE SYSTEM POLICY

APPROVED BY: Andi Diamond, Chief Executive

Officer Date: 15/11/2018

Review Date: 15/11/2020

Issue No: 1

Signature:  _____

Table of Contents

Table of Contents.....	2
1. Definitions and Abbreviations.....	3
2. Acknowledgments.....	4
3. Monash City Council Policy and Reference Documents	4
4. Introduction to the Policy	5
5. Purpose of the Policy	5
6. Policy Parameters/Scope	5
7. Policy Implementation	6
7.1 Practice Principle One: Installation, Privacy and Public Interest	6
7.2 Practice Principle Two: Responsibilities and Accountability	7
7.3 Practice Principle Three: Public Information and Community Consultation	9
7.4 Practice Principle Four: Management of CCTV Monitors	10
7.5 Practice Principle Five: Security, Storage and Access to Data	10
7.6 Practice Principle Six: Maintenance	12
7.7 Practice Principle Seven: Evaluation	13
7.8 Practice Principle Eight: Complaints Process	13

1. Definitions and Abbreviations

CCTV - Closed Circuit Television

CCTV Surveillance System – Council owned and operated surveillance systems in which a number of cameras operate individually and/or collectively connected through a closed circuit. CCTV systems consist of cameras, monitors, recorders, interconnecting hardware and support infrastructure

CCTV Surveillance System Central Register – Central record of all information and relevant data pertaining to the operations and management of any Council owned and operated CCTV Surveillance System

Council buildings and facilities - Any Council civic facility or Council managed public building or facility for use by council staff

Data – Data obtained by Council from a CCTV Surveillance System including (but not limited to) records, film footage, recording, still images or live feeds

IPP – Information Privacy Principles, set out in Schedule 1 of the Privacy and Data Protection Act 2014 (Vic)

Monash City Council Audit & Risk Committee - The Council committee for the ongoing management of audit and risk related matters. A function of the committee will be to uphold the integrity of Council CCTV Surveillance Systems

Monash CCTV Internal Review Committee – The committee established by Council to oversee the installation and operation of CCTV systems. The committee ensures that the operations of Councils CCTV Systems continue to comply with the Policy protocols and privacy requirements

Public Place – Refers to any Council owned and managed CCTV Surveillance System operating in any Council civic facility or Council managed community building, facility or land accessible by council staff and members of the public

Responsible Officer – A Monash City Council staff member involved in the management of a CCTV Surveillance System.

Site-specific Operating Procedures – site specific operational procedures provide instructions on all aspects of the operation and management of Council CCTV Surveillance Systems to ensure compliance with the Policy and consistency of practice

2. Acknowledgments

In developing this Policy, Council referred to the following Acts, Legislation and Standards:

- Charter of Human Rights and Responsibilities Act 2006 (Vic)
- Freedom of Information Act 1982 (Vic)
- Privacy and Data Protection Act 2014 (Vic) ('PDPA 2014')
- Surveillance Devices Act 1999
- Standards Australia – Australian CCTV Standards (2006)

In developing this Policy, Council referred to the following public documents:

- City of Sydney *Street Safety Cameras Program Code of Practice*, 2017
- Commissioner for Privacy and data Protection *Guidelines to Surveillance and Privacy in the Victorian Public Sector*, May 2017
- Guidelines to Surveillance and Privacy in the Victorian Public Sector – Commissioner for Privacy and Data Collection – May 2017
- Whitehorse City Council *CCTV in Public Places Policy*, 2014
- Wollongong City Council *CCTV Policy and Code of Practice*, 2017
- Victorian Auditor General Office (VAGO) report *Security of Surveillance Technologies in Public Places*, September 2018.

3. Monash City Council Policy and Reference Documents

- Business Technology – Non Employee Network Access Policy
- Business Technology – Non Employee Network Access Confidentiality Agreement
- Business Technology – Standard Operating Environment Policy
- Community Consultation and Engagement Policy and Guidelines
- Freedom of Information – Request for Access to Documents
- Privacy Policy and Procedures February 2015

4. Introduction to the Policy

Monash City Council currently operates and manages seventeen (17) fixed CCTV Surveillance Systems within Council facilities and open space (Refer Appendix 1). The role of the CCTV Surveillance System is primarily to ensure public safety, more effectively manage risk and/or to protect council assets. The location of these systems is detailed in Appendix 1.

With the exception of the CCTV Surveillance Systems at the Monash Operations Centre and Monash Waste Transfer Station which monitors footage live, all other Council surveillance systems are re-active where data is recorded and stored for reviewing at a later date as required. Monash City Council does not operate any public safety systems installed in public spaces for specific use by Victoria Police.

Furthermore, Council also manages three (3) solar mobile CCTV camera that specifically target dumped rubbish hotspots.

5. Purpose of the Policy

Monash City Council has primary responsibility for compliance, maintenance, management and security of Council owned and operated CCTV Surveillance Systems. Council must fulfil their responsibility ensuring individuals' right to privacy are maintained at all times, by managing these systems in compliance with privacy requirements.

The purpose of the Monash City Council CCTV Surveillance System Policy (**the Policy**) is to:

- provide a framework to inform and guide decision making on the implementation, installation, data management and operation of any fixed and mobile camera system;
- assist Council to regulate the operation and management of Council-owned CCTV systems installed and operating (or which in the future may be installed) in public places in accordance with best practice, relevant legislation and other laws;
- ensure that the management of CCTV data inclusive of any footage, images, records or the observation of live feeds is appropriate in respect to (amongst other considerations) the use, retention, security, privacy access, disclosure, storage and disposal of data;
- ensure there are appropriate audit evaluation and reporting systems and complaint handling processes; and
- ensure Council staff working with Council CCTV Surveillance Systems undertake their duties in accordance with this Policy supplemented by any Site-specific Operating Procedures and the PDPA2014.

6. Policy Parameters/Scope

This Policy relates to Council owned CCTV Surveillance Systems installed, operated and monitored by or on behalf of Council in and around Council land, buildings and facilities for the purposes of staff and public safety and asset protection.

CCTV Surveillance Systems may also be installed from time to time by lease or licence holders of Council land or buildings as a separate safety measure by the licensee. Whilst remaining the sole responsibility of the lease or licence holder, full compliance with the Monash City Council CCTV Surveillance System Policy is required (excluding reporting and audit requirements).

This Policy does not relate to mobile cameras such as dash cams and body worn video cameras that are primarily used for Council activities associated with enforcement by authorised officers of Council in their delegated tasks or for personal safety. Council owned and managed CCTV Surveillance Systems will not be used to record or monitor the daily activities of Council employees.

7. Policy Implementation

7.1 Practice Principle One: Installation, Privacy and Public Interest

Monash City Council's CCTV Surveillance Systems are installed for proper and lawful purposes in accordance with the Policy. Public interest in the operation of the CCTV Program will be recognised by ensuring the security and integrity of operational procedures. All installations will require a privacy impact assessment to be undertaken by the responsible Officer prior to their use or continued use. Councils Privacy Officer can provide the required guidance to inform the development of all privacy impact assessments.

7.1.1 Installation: Council owned and operated buildings, facilities and land

The use of CCTV Surveillance Systems (fixed or mobile) will need to be authorised by the Monash CCTV Internal Review Committee prior to installation. Applications will need to detail (amongst other matters):

- The relevant function or activity that the implementation of the CCTV Surveillance System is required to facilitate with consideration being given to Information Privacy Principle 1 (IPP1);
- the issue/risk to be mitigated through the use of CCTV surveillance;
- why CCTV surveillance is considered the best option;
- whether other crime prevention through environmental design (CPTED) considerations are more applicable;
- whether the benefits of the surveillance substantially outweigh any invasion of privacy;
- length of installation (permanent or temporary);
- what information is to be collected and how and where it can be used and stored;
- the impacts on the privacy of individuals and groups via a privacy impact assessment;
- the availability of supporting infrastructure and/or feasibility of installing additional infrastructure;
- community consultation undertaken including a full summary of the outcomes;
- human rights considerations;
- governance, monitoring, operating and reporting arrangements;
- if the CCTV Surveillance System is able to be calibrated to avoid over-collection of personal information; and
- the cost and availability of funding for the installation, maintenance and monitoring.

The Monash City Council CCTV Application Proforma is detailed in **Appendix 2**.

7.1.2 Installation: Community Groups in Council owned buildings, facilities and land

This approval process will also be applicable for the installation of CCTV Surveillance Systems proposed by community groups in Council owned buildings under an exclusive user lease or licence arrangement. This approval process will ensure that community accessing any Council building and/or facility where CCTV Systems operate can be assured that their privacy is protected and that CCTV Surveillance System fully complies with all relevant legislation and Council Policy, excluding reporting requirements to Council and the Audit and Risk Committee.

7.1.3 Exclusions

To avoid unwarranted intrusion into privacy, CCTV Surveillance Systems will not be installed:

- in predominantly residential areas or where CCTV cameras may overlook residential properties; and
- in sporting reserves which the community can access for personal fitness, health and wellbeing unless sanctioned by Council for the purpose of asset protection, (for example Jack Edwards synthetic pitch).

7.2 Practice Principle Two: Responsibilities and Accountability

Councils Chief Operating Officer has prime responsibility for ensuring the Policy is adhered to on behalf of Monash City Council. This responsibility includes ensuring compliance with the Policy and all relevant legislation and that any breaches of the Policy are investigated and remedied.

The Chief Operating Officer will retain records of all existing new, additional, altered or removed cameras including the reasons why, in the CCTV Surveillance System central register. This record will also include the site-specific operating procedures for all Council owned and operated systems.

7.2.1 Monash Internal Review Committee

The Monash CCTV Internal Review Committee is responsible for ensuring the operations of the CCTV Surveillance Systems continues to be for designated purposes only, compliance with the Policy and privacy requirements and all relevant legislation.

The Monash CCTV Internal Review Committee will:

- make decisions regarding the installation and decommissioning of any CCTV Surveillance System;
- ensure full compliance with the Policy and any relevant legislation through monitoring, audits and annual reporting;
- conduct an annual review of all site-specific operational procedures and endorse any variations or amendments;
- review this Policy and make amendments to ensure full compliance with all relevant legislation; and
- present an annual operational report to the Audit and Risk Committee which will thereafter be published on the Monash City Council website.

The internal review committee has the right of inspection of all CCTV facilities, procedural documentation, files, registers and records. The Monash CCTV Internal Review Committee is to receive formal notification of any incident and/or request for data within 24 hours of the occurrence or request and then receive a report of the outcome once resolved.

Membership of the Monash CCTV Internal Review Committee will include:

- Chief Operating Officer (chair);
- Coordinator Neighbourhoods and Place Making;
- Coordinator Legal Services;
- Manager Strategic Asset Management; and
- Director of Community Services and Development.

This composition of the Monash CCTV Internal Review Committee will be reviewed annually.

7.2.2 Management Reporting

The Monash CCTV Internal Review Committee is required to formally report to the Audit and Risk Committee on an annual basis detailing (amongst other matters):

- the sites of Council and operated CCTV Surveillance Systems noting any changes to this list or replacement of equipment;
- the sites of CCTV Surveillance Systems operating in Council buildings and land operated under a lease or licence arrangement with a community group noting any changes to this list or replacement of equipment;
- the number of incidents requiring review or access to CCTV data made by Council or enforcement agencies;

- the number of requests under FOI for access to CCTV data including the number of times data has been released, the type of data released by Councils Privacy Officer;
- the number of complaints; and
- a summary of maintenance issues or any changes to the maintenance regime.

The annual report will be made publicly available on Council's website.

To inform the annual report, Responsible Officers are required to provide a monthly and annual report to the Monash CCTV Internal Review Committee using the reporting proforma detailed in **Appendix 3**.

7.2.3 Audit and Risk Committee

A compliance audit will be conducted by Monash City Council's Internal Auditors every second year. The audit will review compliance against the Policy parameters for mobile and fixed systems and make recommendations for future improvements. This Audit will be presented to the Monash City Council Audit and Risk Committee.

It should be noted that the Monash Internal CCTV Review Committee will conduct a review every alternate year with Year 1 commencing 2019.

7.2.4 Responsible Officers

Responsible Officers will oversee the technical and operational matters pertaining to a particular site where a Council CCTV Surveillance System operates. Responsible Officers are accountable for ensuring the development and review of the site-specific operational procedures are in accordance with the Policy and relevant legislative requirements.

To ensure the integrity of the Policy, Responsible Officers will be formally appointed by the Monash Internal CCTV Review Committee.

7.2.5 Site Specific Operational Procedures

The development of Site-Specific Operating Procedures will ensure that the privacy of individuals is protected and that Council CCTV Surveillance Systems are used for their designated purpose only. Council officers designated to operate and oversee a Council CCTV Surveillance System are accountable under this Policy and the PDPA2014.

Site-Specific Operating Procedures provide detailed instructions on all aspects of the operation and management of Council CCTV Surveillance Systems to ensure compliance with the Policy and consistency of practice. In the development of the operational procedures, consideration will need to be given to the following:

- documentation of technical aspects of the system including maintenance regimes to ensure effective operations of the system including the specific arrangements with any external maintenance contractors with regards to privacy and data security;
- operation and management protocols to ensure integrity and compliance with all relevant legislation, standards, codes and guidelines as outlined in this Policy including due consideration to the privacy and respect for the human rights of members of the public;
- operating protocols and procedures relating to the:

- ongoing monitoring, reporting and annual evaluation regimes to ensure compliance with all Policy parameters
- storage and retention of CCTV Data and the monitoring of live feeds (refer Practice Principle 5: Storage and Access to Data);
- requests for access or to view CCTV Data (refer Practice Principle 5: Storage and Access to Data);
- incident escalation and reporting;
- quarterly and annual reporting requirements;
- complaints procedure (Refer Practice Principle 6); and the
- maintenance of an electronic site log book (via Councils corporate data management system) to record any incidents, requests for information and complaints.

All Site-Specific operating procedures are to be completed using the standard format (refer Appendix 4) and then securely stored on site and provided to the Chief Operating Officer for storage on the CCTV Surveillance System.

7.2.6 Training and Staff Responsibilities

All Responsible Officers and members of the Monash Internal Review Committee must understand the contents of the Policy, and are required to sign an acknowledgement of their understanding.

All Responsible Officers will undergo privacy training on an ongoing basis to ensure awareness of the obligations under the PDPA2014, internal policy parameters and other relevant legislation. The training will ensure a consistent approach and practice within the organisation to protecting personal information. Training will be inclusive of (but not limited to) all relevant legislation, Policy parameters and include any key areas identified by the Victorian Information Commissioner on how to use, store, disclose and dispose of recorded surveillance data, probity principles and confidentiality.

7.2.7 Responding and Recording Incidents

The Responsible Officer is required to maintain a site log book to record any incidents, requests for information and complaints. They must formally notify the Monash CCTV Internal Review Committee of any incident and/or request for data within 24 hours of the occurrence or request and receive a report once concluded.

7.3 Practice Principle Three: Public Information and Community Consultation

The public will be provided with clear and easily accessible information in relation to the operation of Monash City Council CCTV Systems. Copies of the Monash City Council CCTV Surveillance System Policy will be made available to the public on Council's website.

7.3.1 CCTV Signage

Signs advising that CCTV cameras are operating will be clearly displayed at the entrance/s of all Council buildings and land and at other key points as deemed site appropriate by the Monash Internal Review Committee. These signs will:

- inform the public that CCTV surveillance cameras are in operation;
- identify that footage is either being constantly recorded or recorded and monitored; and
- identify Monash City Council as the owner of the CCTV Surveillance System and provide contact details should further information be required.

To ensure consistency across all Council buildings and land, the following CCTV Signage wording will be used:

CCTV IN OPERATION

Images are being [monitored and] constantly recorded by Monash City Council for the purposes of [insert purpose eg. Public safety].

For further information please contact Monash City Council on 03 9518 3555.

www.monash.vic.gov.au/cctv

In Council buildings used for administration and operations, appropriate signage will be displayed at all sites and below each camera within those areas, to inform Council staff, Councillors and the public of the use of cameras for security purposes. The cameras will not be used to record or monitor the daily activities of Council employees.

7.3.2 Consultation

The proposed installation of CCTV Surveillance Systems or their removal, will require community consultation and the development of a community consultation strategy as per Councils Community Consultation and Engagement Policy. Consultation with the relevant Council Advisory Groups, Victoria Police (as appropriate) and other key stakeholder such as residents, traders and/or user groups is to be undertaken in accordance with each consultation plan. Exemptions to undertaking community consultation may be granted by the Monash CCTV Internal Review Committee under exceptional circumstances, such as addressing public risk issues consistent with Council's Community Consultation and Engagement Policy and Guidelines.

7.4 Practice Principle Four: Management of CCTV Monitors

Responsible Officers who have responsibilities in relation to the control of CCTV monitors will meet and apply the highest standards of probity and confidentiality to maintain and protect personal information. Access to monitors will be restricted to Responsible Officers who have been appropriately trained and identified in each Site-Specific Operating Procedure. All Responsible Officers involved in the operation of a Council CCTV Surveillance System and members of the Monash CCTV Internal Review Committee are required to sign a confidentiality agreement prior to accessing any Council system.

7.5 Practice Principle Five: Security, Storage and Access to Data

All Monash CCTV network recording or digital recording systems will be securely stored and housed in racks or cabinets that are segregated from the main work area and designed to provide physical and climatic protection suitable to host data storage equipment to avoid loss of data due to possible system failure. To restrict unauthorised access, all CCTV Surveillance System storage areas are only assessable to the Responsible Officers, the Chief Operating Officer, Coordinator Legal Services or Manager Business Technology.

7.5.1 Live Feed Monitors

Live feed monitors will be located in secure areas that are not visible by non-authorised Council staff or members of the public.

In locations where CCTV camera vision may be viewed by unauthorised staff, Council is to ensure that Responsible Officers have an awareness of the privacy requirements and the importance of ensuring confidentiality and appropriate access to data and to minimise the opportunities for inadvertent viewing by others.

7.5.2 Recording Monitors

Responsible Officers who have obligations in relation to controlling CCTV Surveillance System monitors that record data, will need to ensure that they are operated in strict accordance with this Policy and that access to the data and equipment is secure and appropriately housed to restrict unauthorised access.

7.5.3 Security - BT Access Controls

To ensure data security and protect against privacy breaches, the following controls will be implemented:

- Key access controls for CCTV Surveillance Systems include restricting user and administrative access, enforced use of secure passwords and the performing periodic user access reviews and monitoring access to the system regularly;
- Controlled system access via Access Control Lists (ACL) will be maintained to ensure that only Responsible Officers can access the live or recorded CCTV footage;
- Scheduled patching of CCTV Surveillance Systems will be undertaken by Council's Business Technology team to reduce the risk of security vulnerabilities, which could be subject to malware and virus attacks; and
- All CCTV data will be backed up or replicated on a regular basis to ensure data is securely available if there is a system outage or failure, or loss of data.

7.5.4 Breaches

Reports of any inappropriate use and privacy breaches (inadvertent or deliberate) will be reported to the Monash CCTV Internal Review Committee for investigation. This investigation will be in accordance with Council's Privacy Policy. Once the investigation has been completed by Council's Privacy Officer, the Coordinator Legal Services will prepare a report and make recommendations to the Monash CCTV Internal Review Committee for rectification where it is found that a breach did occur.

The Chief Operating Officer will be responsible for maintaining a record of all breaches in the CCTV Surveillance System Central Register. Councils Audit and Risk Committee will be notified of any breach and the action taken to address such breaches via the annual report.

7.5.5 Storage of Data

The retention of, and access to, recorded material will be only for the purposes provided by this Policy or applicable legislation. Recorded material will be retained for up to thirty (30) days unless required in relation to the investigation of a crime and/or for court proceedings. After 30 days they will be recorded over. Recorded data must only be used for the purposes of investigating and providing evidence of an incident.

7.5.6 Access to Data

To ensure privacy and data security obligations are maintained, all requests for access to data must be made to the Chief Operating Officer in writing with a rationale for that request. Responsible Officers are able to download and view data only after written authorisation from the Chief Operating Officer (or Coordinator Legal Services in his/her absence) has been granted.

Data relating to an incident may be disclosed to Victoria Police in accordance with IPP2 or as otherwise authorised by law. Access to data from Council's CCTV Surveillance Systems by Victoria Police has been formalised via a Memorandum of Understanding (MOU) between Council and the Police in accordance with this Policy. Requests are to be made to the Chief Operating Officer and/or Coordinator Legal Services.

Any request by members of the public to view data/records of incidents must be done through the Freedom of Information (FOI) process, as is required to access any Council record. Requests for information must be made using the Monash City Council Freedom of Information – request for Access to Documents form via the Council web link: <https://www.monash.vic.gov.au/About-Us/Council/Governance/Policies-and-Procedures/Freedom-of-Information>

Council will take all reasonable steps to protect data gathered through CCTV systems in public places from misuse and inappropriate disclosure. Release of information to a third party will be done with the strictest scrutiny and in accordance with the purpose of the collection and in accordance with Councils FOI process and the IPP2.

The Chief Operating Officer will maintain a record of all requests for footage, as well as the response in the CCTV Surveillance System Central Register.

7.6 Practice Principle Six: Maintenance

Maintenance of the CCTV Surveillance Systems is undertaken as follows:

- Daily diagnostic checks on cameras and recorders that are connected to the centralised system;
- Weekly visual checks on cameras on all sites;
- Annual maintenance on the systems including:
 - Cameras checked for cracks, damage and stability on supports;
 - Memory cards replaced;
 - Communications and cabling between devices are checked;
 - Cabinets are secured and locked;
 - Software controlling the system is up to date and is functioning as intended;
 - The backup management systems are functioning; and
- All defects identified in the checks are scheduled for repair and undertaken as quickly as practicable.

Staff and contractors undertaking any of the above activities must be trained in application of this Policy and have signed a confidentiality agreement prior to accessing the systems to undertake maintenance works.

A register of all systems is maintained and maintenance actions on each system is recorded. The replacement value of each system is also recorded.

A rolling program of system replacement has also been put into place to maintain the integrity of the systems and ensure that the systems are fit for purpose and meet current standards. In the scoping of new or replacement systems, the following is applied:

- CCTV storage devices hosted in a secured rack or cabinet;
- The rack or cabinet is situated in a space segregated from the staff workspace accessible only by authorised personnel identified above in PP5 under the "Access to Data" section; and
- The location of the rack or cabinet is also to be in a climate controlled environment away that minimises the risk of equipment failure and data loss.

7.7 Practice Principle Seven: Evaluation

Evaluation of the Monash CCTV Surveillance System Policy will be undertaken to identify whether the purposes of the Policy are being fully complied with and meeting its stated purpose and practice principles.

The Chief Operating Officer will lead an evaluation of the CCTV Program every two (2) years, alternate to the Audit and Risk Committee review. The evaluation review will ensure that the Responsible Officer at each location is complying with the Monash City Council CCTV Surveillance System Policy. The primary functions of the evaluation review will include:

- the identification and reporting of any deviations from the Policy or Site-specific Operating Procedures that come to notice;
- ensuring that all Site-specific Operating Procedures are reviewed annually and are consistent with the Policy; and
- recommending actions that will safeguard and enhance the CCTV Surveillance Systems.

The scope of the evaluation will be developed by the Monash CCTV Internal Review Committee in consultation with Councils Audit and Risk Committee.

The results of the evaluation will be made available for public information upon request and on Council's website.

7.8 Practice Principle Eight: Complaints Process

The Monash City Council CCTV Surveillance System Policy will be available to the public to allow scrutiny of operational consistency with policy document.

Enquiries/Complaints

Complaints in relation to any aspect of the management or operation of the system may be made in writing to:

Chief Executive Officer
Monash City Council
293 Springvale Road Glen Waverley VIC 3150
Email: mail@monash.vic.gov.au
Telephone on (03) 9518 3555

The Chief Executive Officer will refer all complaints to the Monash CCTV Internal Review Committee for investigation.

Complaints in relation to Privacy should initially be made to Council's Privacy Officer in accordance with Councils Privacy Policy. Alternatively, a complaint can be made in writing to the Victorian Information Commissioner to:

Office of the Victorian Information Commissioner
PO Box 24274
Melbourne VIC 3001
Email: enquiries@ovic.vic.gov.au

Monash City Council will fully cooperate with the investigation of any complaint received from the Victorian Information Commissioner.

APPENDIX 1: Monash City Council CCTV System Locations

LOCATION	PRIMARY PURPOSE/S FOR INSTALLATION	NUMBER OF CAMERAS	RESPONSIBLE OFFICER
Glen Waverley Civic Centre ¹	Public safety Risk Management	19	Manager Business Technology
Oakleigh Service Centre	Public safety Risk Management	3	Manager Business Technology
Monash Training and Seminar Centre	Public safety Risk Management	1	Manager Business Technology
Monash Waste and Transfer Station ¹	Security of assets Public safety Risk Management	13	Manager Sustainable Monash
Monash Operations Centre ²	Security of assets Public safety Risk Management	28	Manager Strategic Asset Management
Clayton Community Centre	Security of assets Public safety Risk Management	47	Manager Business Technology
Monash Gallery of Art	Security of assets Public safety Risk Management	38	Director Community Development & Services
Wheelers Hill Library	Security of assets Public safety Risk Management	6	Manager Community Support and Libraries
Mount Waverley Library	Security of assets Public safety Risk Management	6	Manager Community Support and Libraries
Oakleigh Library	Security of assets Public safety Risk Management	9	Manager Community Support and Libraries
Glen Waverley Library	Security of assets Public safety Risk Management	6	Manager Community Support and Libraries
Monash Recreation and Aquatics Centre	Public safety Risk Management	34	Manager Active Monash
Oakleigh Recreation Centre ²	Public safety Risk Management	18	Manager Active Monash
Batesford Community Hub	Public safety Risk Management	8	Manager Business Technology
Euneva Car Park	Public safety	24	Manager Strategic Asset Management

Atkinson Street Car Park	Public safety	18	Manager Strategic Asset Management
Jack Edwards Reserve Synthetic Pitch ³	Security of assets	4	Manager Strategic Asset Management

Notes:

1. Inclusive of the three CCTV surveillance cameras at IBIS (295 Springvale Rd, Glen Waverley)
2. Live Feed CCTV System
3. CCTV System externally monitored through contract arrangements with Wilson Security

In addition, Council operates and manages three (3) single camera solar powered portable CCTV systems.

Monash City Council CCTV Surveillance System - Appendix 2



APPLICATION FORM FOR THE INSTALLATION OF A CCTV SURVEILLANCE SYSTEM ON COUNCIL OWNED BUILDINGS AND LAND

The Monash City Council Application to Install a CCTV Surveillance System Proforma is to be used by Council staff or community groups under a lease and licence arrangement with Council seeking to install a fixed or mobile CCTV Surveillance System. The completed application is to be forwarded to the Monash Internal Review Committee for assessment. To ensure integrity and compliance, a CCTV Surveillance System cannot be operated until approval is granted by the Monash CCTV Internal Review Committee.

Name of Applicant:

Relevant function/activity that the implementation of the CCTV Surveillance System is required to facilitate with consideration given to IPP1:

Issue/risk to be mitigated through the use of CCTV Surveillance System:

Why CCTV surveillance is considered the best option:

What CCTV Surveillance System is being proposed to be installed. Is the system able to be calibrated to avoid over-collection of personal information?

What other crime prevention through environmental design (CPTED) considerations are in place?

How the benefits of the surveillance outweigh any invasion of privacy:

Length of installation (permanent or temporary):

Privacy Impact Assessment (inclusive of human rights considerations):

What information is to be collected and how and where it can be used and stored:

Assessment of the supporting infrastructure including feasibility of installing additional infrastructure:

Community consultation undertaken. Please attach a full summary of the outcomes):

What governance, monitoring, operating and reporting arrangements are proposed:

- *How will the system be monitored*
- *Where will monitors be located (if required)*
- *What is the process for managing requests for footage*
- *Process for accessing footage and who will be delegated to undertake this to protect the privacy of individuals*

What maintenance regimes are required:

- *Who will undertake this and what privacy consideration will be in place*

Cost and availability of funding for the installation and maintenance:

Monash City Council CCTV Surveillance System - Appendix 3



Monthly/Annual Report

Site/Location:

Date:

Name of Responsible Officer:

Number of incidents requiring review of CCTV data

Detail the type of data requested, incident, reason for viewing, who authorised access, person who viewed data.

Number of requests under FOI of CCTV data

Detail the number of times data has been released, the reasons and who authorised this release:

Number of complaints

Reason and outcome/resolution:

Summary of maintenance issues

Detail type of issue, impact to the system and length of time to resolve:

Summary of any additional operational issues including any breach (or potential) of privacy or system security:

Monash City Council CCTV Surveillance System - Appendix 4



SITE-SPECIFIC OPERATIONAL PROCEDURES

Responsible Officer/s:

Purpose of the CCTV Surveillance System surveillance:

Type of CCTV System and Key Technical Aspects:

Privacy Impact Assessment:

Signage location/s:

Specifications as to how the information is to be collected and stored:

Relevant legislation that governs the CCTV Surveillance System:

The roles and responsibilities for the management of the CCTV Surveillance System:

The protocols for ensuring the security of information:

ICT controls are in place to prevent unauthorised access to the system and footage:

Storage arrangements to ensure that the system is securely stored:

Type of information/data being captured and stored:

Length of time information/data will be stored:

Incident escalation and reporting protocols:

Permissions to access the information and procedure for this to occur:

Site specific process for accessing data or requests for data:

Maintenance regime and process for reporting system issues to ensure effective operations:

Specific arrangements and formal agreements for external maintenance contractors with regards to privacy and data security:

Process for managing complaints and privacy breaches:

Reporting, evaluation and audit arrangements:

Process to ensure the maintenance of a Log Book to record any incidents, requests for information and complaints – location and reporting arrangements: