

# Closed Circuit Television Policy

<b>Date first adopted:</b>	22 July 2014
<b>Dates amended:</b>	3 February 2015 25 February 2020
<b>Next review date:</b>	
<b>Position title of responsible business unit Manager:</b>	Corporate Counsel
<b>Approved by:</b>	Council

## CONTENTS

1. TITLE .....	3
2. OBJECTIVE.....	3
3. DEFINITIONS AND ABBREVIATIONS.....	3
4. POLICY.....	3
5. HUMAN RIGHTS CHARTER COMPATIBILITY.....	5
6. ASSOCIATED DOCUMENTS .....	5
7. REFERENCES/RESOURCES .....	5

## 1. TITLE

Closed Circuit Television Policy

## 2. OBJECTIVE

To set out Council's policy:

- for the installation and use of closed circuit television (CCTV) on properties and facilities which are owned or controlled by Council; and
- for the collection, access, storage and disposal of data obtained by Council from a Council CCTV system

in accordance with relevant laws and standards.

## 3. DEFINITIONS AND ABBREVIATIONS

Term	Meaning
CCTV	Closed Circuit Television.
CCTV Data	Data obtained by Council from a Council CCTV System, including film footage, recordings and still photographs.
CCTV Management Officer	A Council officer nominated to perform day-to-day maintenance as required on the Council CCTV System, or respond to a request for CCTV Data under this policy
Corporate Counsel	The senior officer responsible for leading the Corporate Counsel department, or any person acting in this position.
Council assets	includes any land, building or infrastructure owned, managed or occupied by Council
Council CCTV System	A surveillance system consisting of: <ul style="list-style-type: none"><li>• cameras connected through a closed circuit and transmitting signals to specific television monitors or recorders ; and</li><li>• interconnecting hardware and support infrastructure</li></ul> which is installed and used on properties and facilities owned or controlled by Council.
Facilities Staff	Staff with responsibility for the maintenance or management of a Council asset or facility, and have been nominated by their manager for permission to view live CCTV footage for that asset or facility.

## 4. POLICY

### General

- 4.1 In line with the Council and Community Plan, Council provides and manages services, assets and facilities for the benefit of the community.
- 4.2 Council owns and operates the Council CCTV System, including live CCTV cameras, to support the provision and management of Council services, assets and facilities.
- 4.3 Council does not operate any CCTV cameras or systems in privately owned buildings or properties, or for

the enforcement of criminal law.

#### **Installation of Council CCTV cameras**

- 4.4 A Director or the Chief Executive Officer may approve locations where a new Council CCTV camera will be installed in consultation with internal stakeholders.

#### **Operation of Council CCTV Systems**

- 4.5 The following persons are responsible for maintaining the Council CCTV System and ensuring that it is operated in accordance with applicable laws, regulations, standards, policies and procedures:
- (a) the Manager of Glen Eira Leisure, in relation to CCTV cameras installed in Glen Eira Leisure facilities; and
  - (b) the Manager of Buildings, Properties and Planning Enforcement, in relation to CCTV cameras installed in all other Council facilities.
- 4.6 The responsible Manager described in section 4.5 will ensure that signs are displayed at the perimeter of the area recorded and at other key points as determined by Council from time to time. The signs will:
- (a) identify Council as the owner of the CCTV camera;
  - (b) contain words or symbols which make it clear that Council operates CCTV cameras, and individuals or activities in or around the area may be recorded; and
  - (c) provide contact details for any enquiries relating to the Council CCTV System.

#### **Access to live CCTV Data**

- 4.7 Staff with responsibility for the maintenance or management of a Council asset or facility (**Facilities Staff**) may view live CCTV cameras as operationally required to effectively carry out their functions or to respond to an actual or reported emergency. Facilities Staff must be nominated by their manager and undertake appropriate training before being permitted to view live CCTV cameras, and are not permitted to access CCTV Data.

#### **Access to recorded CCTV Data**

- 4.8 The responsible Manager described in section 4.5 may nominate CCTV Management Officers to perform day-to-day maintenance as required on the Council CCTV System, or respond to a request for CCTV Data (including by seeking approval to provide access to CCTV Data), and is responsible for ensuring that any CCTV Management Officer they nominate are appropriately trained to perform their functions in accordance with this policy.
- 4.9 Corporate Counsel (or an officer nominated by Corporate Counsel) may approve a request for access to CCTV Data as follows:
- (a) to a Council employee, contractor or agent, if access is necessary to facilitate the provision and management of Council services, assets and facilities (**internal access**);
  - (b) to a law enforcement authority, if access is necessary to prevent investigate or prosecute a criminal offence or breach of law imposing a sanction (**law enforcement access**); or
  - (c) otherwise as required to comply with a legal obligation.
- 4.10 All requests for access to CCTV Data must be made in writing and:
- (a) in the case of an internal access request, the request must be approved in writing by a Manager or Director; and
  - (b) in the case of a law enforcement access request, the request must include the officer's rank, identification number and station (if a police officer) or position, and state the legislative provision under which an investigation or prosecution is being conducted.

- 4.11 Access to CCTV Data may only be provided without approval from Corporate Counsel in the following circumstances:
- (a) a Manager, Director or the Chief Executive Officer may approve access to CCTV Data if, in the view of the approving Manager, Director or the CEO, access to CCTV Data is reasonably necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare, or a serious threat to public health, public safety or public welfare; or
  - (b) if there is an emergency triggering the Municipal Emergency Management Plan or any relevant sub-plans, the Municipal Emergency Response Officer may approve access to CCTV Data as required to respond to the emergency.

If access to CCTV Data is provided under this clause, the person approving access to CCTV Data must notify Corporate Counsel as soon as practicable after access is provided.

- 4.12 Council will endeavor to provide access to CCTV Data in the form requested, taking into account operational requirements.
- 4.13 Council generally stores CCTV Data securely in the Council CCTV System for a period of 90 days before it is automatically erased. If a request for CCTV Data is approved, the requested CCTV Data may be retained, accessed and used in accordance with the request rather than being automatically erased after 90 days.
- 4.14 Council will keep a written record of requests for CCTV Data in accordance with Council's records management obligations.

## **5. HUMAN RIGHTS CHARTER COMPATIBILITY**

This Policy has been assessed as being compatible with the Charter of Human Rights and Responsibilities Act 2006 (Vic).

## **6. ASSOCIATED INTERNAL DOCUMENTS**

[Glen Eira Council and Community Plan](#)  
[Privacy Policy](#)  
[Health Records Policy](#)

## **7. EXTERNAL REFERENCES/RESOURCES**

[AS 4806 Standards for Closed Circuit Television](#)  
[Charter of Human Rights and Responsibilities Act 2006 \(Vic\)](#)  
[Evidence Act 2008 \(Vic\)](#)  
[Guidance to surveillance and privacy in the Victorian public sector, published by the Office of the Victorian Information Commissioner \(May 2017\)](#)  
[Freedom of Information Act 1982 \(Vic\)](#)  
[Municipal Emergency Management Plan](#)  
[Privacy and Data Protection Act 2014 \(Vic\)](#)  
[Public Records Act 1973 \(Vic\)](#)  
[Surveillance Devices Act 1999 \(Vic\)](#)  
[Health Records Act 2001 \(Vic\)](#)