CCTV Policy

Date Adopted: Tuesday, 26th November 2024

Version: 1.0

Policy Objectives

- Provide direction and guidance to Maitland City Council ('Council') when considering the management and use of closed circuit television (CCTV) in public places or on Council-managed property or infrastructure.

- Ensure that Council CCTV camera network systems comply with relevant statutory requirements.

Policy Scope

This Policy applies to the Council-owned CCTV camera network installed in public places for surveillance purposes. This includes cameras located on Council property and mobile surveillance cameras. With express permission, mobile cameras may also be placed on private land or attached to Council vehicles and equipment.

The installation and placement of CCTV cameras, as well as other aspects of the CCTV system, will be determined solely by the Council in consultation with relevant stakeholders as appropriate.

This Policy is not intended to guide the use of CCTV cameras operated by other parties. This includes private landowners or businesses, as well as tenants or licensees of Council land or buildings, who must only install CCTV cameras in accordance with the terms of their leases or licenses (or with the consent of Council if those are silent on the issue).

This Policy applies to the General Manager, all Council staff, councillors, contractors, volunteers and committees.

Policy Statement

Council considers it important to provide a safe environment for its staff and community. The primary purpose of Closed-Circuit Television (CCTV) camera network is to deter and/or detect unlawful activity and help improve the community's perception of safety.

Council also recognises that CCTV is just one of many strategies to reduce crime. The preferred approach is to use Crime Prevention through Environmental Design principles for any spaces Council designs or constructs. This approach includes creating clear sightlines, minimising concealed areas, installing appropriate lighting, enhancing natural surveillance, increasing access control, and improving signage before considering the installation of CCTV.

The development of this Policy has been guided by the *NSW Government Policy Statement and Guidelines for the Establishment and Implementation of Closed-Circuit Television (CCTV) in Public Places*.

Council is dedicated to safeguarding the privacy of individuals by ensuring that any personal information or health information collected within the CCTV camera network follows the *Privacy and*

Personal Information Protection Act 1998 (NSW) and the *Health Records and Information Privacy Act 2002* (NSW).

Council's CCTV camera network will not be used for the purposes of automated biometric verification or biometric identification such as facial recognition.

Council will comply with the requirements of the *Surveillance Devices Act 2007* generally and in particular in relation to any audio captured on the CCTV camera network (which is only captured in very limited locations and very limited circumstances with appropriate signage).

Council will regularly evaluate the CCTV camera network to determine whether it is achieving its objectives.

Collection of Information

Council currently operates a CCTV camera network in the area around Maitland Administration Centre, Maitland Resources Recovery Facility, Maitland Regional Athletics Centre, Maitland Regional Art Gallery, Maitland City Council Works Depot and Maitland Animal Management Facility. Live feeds from the Maitland Administration Centre are monitored by Council authorised staff. Council also has CCTV installations on mobile equipment and at numerous public locations throughout the local government area.

When the Council collects CCTV camera footage, it will be:

- managed in accordance with the Privacy and Personal Information Protection Act 1998, Health Records and Information Privacy Act 2002, Government Information (Public Access) Act 2009, Workplace Surveillance Act 2005, and the NSW Local Government Act 1993.
- managed according to the Council's Privacy Management Plan.
- managed in compliance with the legal obligations under the Information Protection Principles (IPP) and Health Protection Principles (HPP) for collection, storage, use, and disclosure.
- subject to the NSW Mandatory Notification of Data Breach (MNDB) Scheme.

These steps ensure that CCTV footage is handled responsibly and in compliance with legal requirements.

Use and Disclosure

Council will ensure that the CCTV camera network is only used for the purposes for which it was collected or as otherwise permitted by law. It will not be used for general intelligence gathering purposes.

Council will not disclose CCTV footage or photographs generated from the footage or any accompanying audio to third parties without the individual's consent, except where required by law or where necessary to lessen or prevent a threat to life, health or safety.

Governance

The use of CCTV within the Maitland City Local Government Area will be operated fairly and transparently, in accordance with applicable laws.

The Council retains ownership and copyright of all documentation, recorded material, and other materials related to CCTV operations under this Policy.

It is acknowledged that CCTV cameras installed in public place locations and as part of Council infrastructure may also capture Council staff performing work tasks. The CCTV camera network, the subject of this policy, is not designed to intentionally provide workplace surveillance. Where the purpose is to provide workplace surveillance or a record of accidents or other non-crime incidents involving Council staff, Council will comply with the *Workplace Surveillance Act 2005* and will apply Council's Workplace Surveillance Policy , including complying with the notice requirements.

Any proposal to implement the CCTV system at a specific public location will be assessed according to the *Guiding Principles of the NSW Government Policy Statement and Guidelines for the Establishment and Implementation of CCTV in Public Places*.

CCTV Image Monitoring, Capture, Storage, Disposal and Signage

The CCTV system will not be monitored 24 hours a day 7 days a week. It will primarily serve as a tool for law enforcement to address criminal activity and identify offenders, aiming to reduce harm to the community. To achieve this, footage will be captured and recorded. Recordings will be kept securely and for no longer than is necessary for the purposes of this policy.

Recorded material from Council's CCTV camera network is considered a public record and is subject to standard information management security procedures as outlined in the NSW *State Records Act 1998* and the Council's Record Management Policy and Right to Information Policy. Recorded material no longer required will be disposed of using approved disposal methods.

The Council will inform the public through relevant and clearly visible signage when Council CCTV cameras are in operation at a location, including where audio is captured as applicable.

Security

Council will take reasonable steps to ensure that the CCTV footage it collects is accurate, up-to-date, complete and retained in accordance with Council's '*Records Management Policy*'. Council is committed to implementing security measures to protect this information from misuse, loss, unauthorised access, modification, or disclosure.

The Council will implement appropriate security measures and internal controls to prevent unauthorised access, alteration, disclosure, accidental loss, or destruction of recorded material. Only appropriately licensed, trained and authorised personnel will have access to operating controls and recording facilities, except in the case of an emergency when NSW Police or other NSW government agencies may have access with the approval of the General Manager.

Council will ensure the installation of CCTV cameras will be undertaken by persons who are appropriately licensed under the *Security Industry Act 1997*.

Access and Correction

Individuals have the right to request access and change contact details, please refer to Maitland City Councils '*Right to Information Guidelines'* and *'Change of Contact Details'* on our website. All public requests for access to recorded material, must be made through an Access Application pursuant to the *Government Information (Public Access) Act 2009* (GIPA), please visit our '*Governance and Transparency*' section of our website.

Recorded material will not be sold or used for commercial purposes or entertainment. It will only be used for the purposes outlined in this Policy. The display of recorded material to the public will only be permitted in accordance with law enforcement functions related to the investigation of crime, missing person, or as allowed by law.

Maintenance

Council will put in place processes to inspect and maintain the CCTV camera network for proper performance to ensure the footage it provides is accurate, up to date and complete. Council will ensure that any person engaging in maintaining the CCTV system is appropriately licensed as required by the *Security Industry Act 1997*

Enquiries and Complaints

Council encourages anyone with an enquiry or concern about its CCTV camera network to first discuss the issues informally with Council's Customer Experience Team via the below contact details.

Contact details:
Email: cet@maitland.nsw.gov.au
Phone: 4934 9700
Live chat: via website: www.maitland.nsw.gov.au
In person: 263 High Street, Maitland NSW 2320

Complaints in relation to Council's establishment, management or operation of CCTV may be made through Council's existing customer complaints processes (verbally or in writing by letter, email, fax or live chat). Complaints, except for those specified below, will be managed in accordance with Council's '*Complaint Management Policy*'.

Complaints or enquiries about the handling of CCTV footage and a person's personal or health information or possible data breaches can be directed to Council's Privacy Officer via the below contact details. Such complaints will be managed in accordance with Council's '*Privacy Management Plan*' and '*Data Breach Policy*'.

Contact details:
Privacy Officer
Maitland City Council
Post: PO Box 220, Maitland NSW 2320
Email: privavy@maitland.nsw.gov.au
Phone: 4934 9700

Policy Definitions

Affected individual	As defined in section 59D of the PPIP Act, an affected individual is an individual: • to whom the information subject to unauthorised access, unauthorised disclosure or loss relates, and • who a reasonable person would conclude is likely to suffer serious harm as a result of the data breach.
Camera	Includes an electronic device capable of monitoring or recording visual images of activities public places.
Closed Circuit Television (CCTV)	Defined as a television system that transmits images on a 'closed loop' basis, where images are only available to those directly connected to the transmission system. The transmission of closed circuit television images may involve the use of coaxial cable, fibre-optic cable, telephone lines, infra-red, wireless and radio transmission systems. A hand held or fixed video recorder is not

	included in this definition unless it is connected to the transmission system.
CCTV camera network	Refers to a Closed Circuit Television (CCTV) system operated council in public places and within council-operated facilities. It excludes privately owned and operated CCTV systems in private places and is distinct from CCTV used solely for council facility management. The primary purposes include enhancing public safety, deterring crime, protecting council assets, and ensuring operational security
Data breach	Data breach means unauthorised access to, or unauthorised disclosure of, personal information or a loss of personal information. Examples of a data breach are when a device containing personal information is lost or stolen, an entity's database containing personal information is hacked or an entity mistakenly provides personal information to the wrong person.
Employee/Staff	A person working for Council, including contractors and volunteers.
Health information	A specific type of personal information which may include information or an opinion about the physical or mental health or a disability (at any time) of an individual. This includes, for example, information contained in medical certificates, information about medical appointments or test results.
Law enforcement agency	Means any of the following: (a) NSW Police Force, (b) A police force or police service of another State or a Territory, (c) The Australian Federal Police, (d) The Police Integrity Commission, (e) The Independent Commission Against Corruption, (f) The New South Wales Crime Commission, (g) The Australian Crime Commission, (h) The Department of Corrective Services, (i) The Department of Juvenile Justice, (j) Any other authority or person responsible for the enforcement of the criminal laws of the Commonwealth or of the State, (k) A person or body prescribed for the purposes of this definition by the regulations.
Loss	Loss refers to the accidental or inadvertent loss of personal information held by Council, in circumstances where is it is likely to result in unauthorised access or disclosure. For example, where a staff member leaves personal information (including hard copy documents, unsecured computer equipment, or portable storage devices containing personal information) on public transport.
Personal information	Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or could be reasonably ascertained from the information or opinion, as defined in section 4 of the PPIP Act. For the purpose of this policy, personal information includes health information within the meaning of the *Health Records and Information Privacy Act 2002*.
Public Place	Defined in the NSW *Local Government Act 1993* and means public reserves, public bathing reserves, public baths or swimming pools,

	public roads, public bridges, public wharfs or public road-ferries, a Crown reserve, or public land (which is any land vested in or under the control of the council, such as car parks).
Serious harm	Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the affected individual. That is, the effect on the individual must be more than mere irritation, annoyance, or inconvenience. Harm to an individual includes physical harm, economic, financial, or material harm, emotional or psychological harm; reputational harm, and other forms of serious harm that a reasonable person in Council's position would identify as a possible outcome of the data breach.
Unauthorised access	Unauthorised access of personal information occurs when personal information that an entity holds is accessed by someone who is not permitted to have access. This includes unauthorised access by an employee of the entity, or an independent contractor, as well as unauthorised access by an external third party (such as by hacking). For example, a staff member browses a fellow employee's personnel record without any legitimate purpose.
Unauthorised disclosure	Unauthorised disclosure occurs when an entity, whether intentionally or unintentionally, makes personal information accessible or visible to others outside the organisation, and releases that information from its effective control in a way that is not permitted by the PPIP Act. This includes an unauthorised disclosure by an employee of the organisation. For example, a staff member accidentally publishes a confidential data file containing the personal information of one or more individuals on the internet.
Unlawful activity	Means an act or omission that constitutes an offence against a law of this State, or the Commonwealth Video Surveillance is defined as surveillance by a closed circuit television system for direct visual monitoring and/or recording of activities on premises or in a public space.

Policy Administration

BUSINESS GROUP:	Customer and Digital Services
RESPONSIBLE OFFICER:	Manager Enterprise Architecture
COUNCIL REFERENCE:	
POLICY REVIEW DATE:	Three (3) years from date of adoption
FILE NUMBER:	118/1
RELEVANT LEGISLATION	Health Records and Information Protection Act 2002 (NSW) Privacy and Personal Information Protection Act 1998 (NSW) Privacy and Personal information Protection Regulation 2019 (NSW) State Records Act 1998 (NSW) Workplace Surveillance Act 2005 (NSW) Security Industry Act 1997 (NSW) Government Information (Public Access) Act 2009 Surveillance Devices Act 2007 Security Industry Act 1997
RELATED POLICIES / PROCEDURES / PROTOCOLS	Privacy Management Plan Records Management Policy Data Breach Policy Code of Conduct Cyber Information Security Policy Workplace Surveillance Policy

Policy History

VERSION	DATE APPROVED	DESCRIPTION OF CHANGES
1.0	TBC	Initial Policy