11.3 Policy Review - Camera Surveillance

REPORT BY THE GOVERNANCE CO-ORDINATOR
TO 18 OCTOBER 2023 ORDINARY MEETING
GOV400103, GOV400047

RECOMMENDATION

That Council:

1. **receive the report by the Governance Co-ordinator on the Policy Review - Camera Surveillance;**

2. **place the draft Camera Surveillance policy on public exhibition for 28 days; and**

3. **adopt the Camera Surveillance policy if no submissions are received through the public exhibition process.**

Executive summary

The Camera Surveillance policy outlines the way in which Council will operate camera surveillance in public areas and how it will be managed, including the security and access to the information collected in line with privacy legislation.

Council does not operate CCTV in conjunction with NSW Police.

Disclosure of Interest

Nil

Detailed report

Council operates a number of camera surveillance devices through the Mid-Western Regional Council local government area. The purchase, installation and use of camera surveillance devices must be approved by the Executive Team. The primary objective of implementing camera surveillance is for the protection and safety of Council assets, including infrastructure and equipment.

It is important to emphasise that camera surveillance is not intended for staff monitoring purposes.

All camera surveillance devices, including dash cams, iPhones, iPads and digital cameras will be operated in accordance with the *Privacy and Personal Information Protection Act 1998*, *Workplace Surveillance Act 2005* and the *Surveillance Devices Act 2007*. Updates to the policy outline the following measures that will be implemented in order to maintain legislative compliance and also to ensure the safety of the personal information of Council staff and the general public:

- Signage will be displayed at the entrance of all areas under camera surveillance, including entry points to Council events to inform individuals that surveillance is in operation and the reason that surveillance is occurring.

- Footage will only be access for legitimate purposes such as investigating security incidents, reviewing footage related to asset protection or law enforcement purposes.
- Footage retrieved through camera surveillance will be stored on a secure drive with only authorised staff having access.

Council's Executive Team has endorsed an internal Camera Surveillance procedure to guide staff on the operation of camera surveillance devices and the use of information collected.

Community Plan implications

Theme	**Good Government**
Goal	An effective and efficient organisation
Strategy	Prudently manage risks association with all Council activities

Strategic implications

Council Strategies
Asset Management Strategy – Surveillance cameras are in place for the protection of Council assets.

Council Policies
- Privacy Management Plan – Information captured by surveillance devices may include the personal information of individuals.
- Access to Information Policy – As the information captured by surveillance devices is a Council record, requests for access to information can be made by an individual where the information relates to themselves or under the *Government Information (Public Access) Act 2009*.
- Asset Management Policy – Surveillance cameras in place for the protection of Council assets.

Legislation
Surveillance Devices Act 2007
Privacy and Personal Information Protection Act 1998
Privacy and Personal Information Protection Regulation 2019
Government Information (Public Access) Act 2009
Local Government Act 1993
Workplace Surveillance Act 2005

Financial implications

Not Applicable

ASHLEIGH MARSHALL
GOVERNANCE CO-ORDINATOR

SIMON JONES
DIRECTOR COMMUNITY

3 October 2023

Attachments: 1. Draft Camera Surveillance Policy.

APPROVED FOR SUBMISSION:

BRAD CAM
GENERAL MANAGER

POLICY

Camera Surveillance

ADOPTED		VERSION NO	1.1
COUNCIL MEETING MIN	CLICK HERE TO	REVIEW DATE	OCTOBER 2027
DATE:	OCTOBER 2023	FILE NUMBER	GOV400047

A prosperous and progressive community

Objective

The Camera Surveillance Policy informs the community of Council's use of camera surveillance devices in public places. The purposes for which Council use camera surveillance in public places are:

- The protection of community assets,
- Recording of Council works and operations,
- Recording for regulatory and compliance investigations and inspections
- Recording of Council functions / events and;
- Staff safety

The Council does not operate a Closed Circuit Television (CCTV) scheme in cooperation with NSW Police. Information about CCTV used by Government agencies in NSW is available by referring to the link below.

http://www.crimeprevention.nsw.gov.au/documents/councils-publications/cctv_guidelines.pdf

Legislative Requirements

- Surveillance Devices Act 2007
- Privacy and Personal Information Protection Act 1998
- Privacy and Personal Information Protection Regulation 2019
- Government Information (Public Access) Act 2009
- Local Government Act 1993
- Workplace Surveillance Act 2005

Related Policies and Plans

- Camera Surveillance Procedure
- Privacy Management Plan
- Access to Information Policy
- Asset Management Policy
- Asset Management Strategy

Policy

Privacy

Council will comply with the Information Protection Privacy Principles outlined in the *Privacy and Personal Information Protection Act 1998* that underpin the minimum requirements of Council when collecting personal information such as camera surveillance footage and images in public places. The Information Protection Privacy Princples can be viewed at https://www.ipc.nsw.gov.au/information-protection-principles-ipps-agencies and are also attached as annexure .

Council must inform the public that camera surveillance is occurring within the Mid-Western Local Government Area. Council will signpost all sites that have fixed camera video surveillance.

Council will also inform people attending Council facilities, functions and events that video recordings or photography is used. Such information may include signage or a statement at the point of ticket sale that surveillance recordings from these facilities or events may be used in promotions undertaken by the Council.

Cameras will not be used to look into adjacent or nearby premises and no sound will be recorded in public places.

Security

Council is responsible for the maintenance, management and security of all surveillance cameras and the protection of the interests of the public. Council staff will follow the internal Camera Surveillance procedure to ensure that access to recorded footage is restricted and protected from unauthorised access and to maintain compliance with the statutory obligations of Government Agencies under the *Privacy and Personal Information Protection Act 1998 (PPIP Act)* and the *Surveillance Devices Act 2007*.

Council Executive staff must approve the purchase, installation and use of surveillance cameras.

As at November 2022 approved use includes:

- Surveillance of Council waste facilities including Waste Transfer Stations
- Surveillance of Council assets that are buildings in public places
- Surveillance of Council assets in Parks (play/exercise equipment, seating, bins etc.)
- Surveillance of Council assets in Libraries
- Surveillance of Council assets, materials and equipment in public areas of council depots and offices.

Authorised Officers vehicle Dash Cams, iPhones, iPads and digital cameras.
Council has established a dedicated local network drive specifically for the storage of camera surveillance data. This drive is secure and routinely backed up. Only the Managers and authorised staff who operate cameras will have access to their Department's folders within this drive for the filing and viewing of surveillance data. Recorded material will only be accessed when an issue has been identified at a location for the purpose of this policy. An exception to this is at the Mudgee Waste Facility where live footage is visible in the weighbridge office for the purpose of inspecting vehicle loads.

The release of camera surveillance data will only be provided to comply with:

- Internal reporting requirements at Executive or Management levels only;
- The requirements of law enforcement agencies in relation to the investigation of crime;
- A subpoena;
- A valid formal request for public information to which Council decides to provide access under section 58 of the Government Information (Public Access) Act 2009.

Complaints

Council's Complaints Policy is intended to ensure complaints are handled fairly, efficiently and effectively. The complaints management system enable staff to respond to issues raised by people making complaints in a timely and cost-effective way, to boost public confidence in the administrative processes and provide information that can be used to deliver quality improvements in the services, facilities, staff and overall handling of complaints.

Council will acknowledge receipt of complaints within fourteen (14) working days and will keep you up to date with the progress of the complaint and provide a date of which we will respond.

Councils Complaints Policy can be found at https://www.midwestern.nsw.gov.au/Council/Policies-plans-and-reporting/Policies/Complaints-Policy

Annexure A

information and privacy commission new south wales

Fact Sheet **Updated May 2020**

Information Protection Principles (IPPs) for agencies

The 12 Information Protection Principles (IPPs) are your key to the *Privacy and Personal Information Protection Act 1998* (PPIP Act).

General information

There are legal obligations which NSW public sector agencies, statutory bodies, universities and local councils must abide by when they collect, store, use or disclose personal information. As exemptions may apply in some instances, it is therefore suggested you contact the Privacy Contact Officer in your agency or our office for further advice.

Collection

1. Lawful

Only collect personal information for a lawful purpose, which is directly related to the agency's function or activities and necessary for that purpose.

2. Direct

Only collect personal information directly from the person concerned, unless they have authorised collection from someone else, or if the person is under the age of 16 and the information has been provided by a parent or guardian.

3. Open

Inform the person you are collecting the information from why you are collecting it, what you will do with it and who else might see it. Tell the person how they can view and correct their personal information, if the information is required by law or voluntary, and any consequences that may apply if they decide not to provide their information.

4. Relevant

Ensure that the personal information is relevant, accurate, complete, up-to-date and not excessive and that the collection does not unreasonably intrude into the personal affairs of the individual.

Storage

5. Secure

Store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use, modification or disclosure.

Access and Accuracy

6. Transparent

Explain to the person what personal information about them is being stored, why it is being used and any rights they have to access it.

7. Accessilble

Allow people to access their personal information without excessive delay or expense.

8. Correct

Allow people to update, correct or amend their personal information where necessary.

Use

9. Accurate

Make sure that the personal information is relevant, accurate, up to date and complete before using it.

10. Limited

Only use personal information for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person's health or safety.

Disclosure

11. Restricted

Only disclose personal information with a person's consent or if the person was told at the time that it would be disclosed, if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.

12. Safeguarded

An agency cannot disclose sensitive personal information without a person's consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

Full text of the Information Protection Principles, can be seen in the relevant sections of the Privacy and Personal Information Protection Act, 1998 available on the Legislation NSW website: www.legislation.nsw.gov.au

If you would like further advice about the IPPs we encourage you to contact us. Before doing so, we suggest you review our Fact Sheet - The Role of the Privacy Commissioner: Consulting the IPC on Initiatives and Projects.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NOTE: The information in this fact sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.