

Closed Circuit Television (CCTV) Standard Operating Procedure

Record No: 21/44752

Version No: 1



Document Title	Closed Circuit Television (CCTV) Standard Operating Procedure
Council Adopted	February 2023
Council Resolution No	43/2023FC
Version Number	1
Responsible Department	Corporate and Community Services
Date to be Reviewed	February 2027

Table of Contents

1. Purpose	4
2. Background	4
3. Scope.....	4
4. Definitions.....	4
5. Responsibilities	5
6. Key Principles	5
7. Risk Management	6
8. System Description, Locations & Purposes.....	7
9. New CCTV Systems	8
10. Standard Operating Procedures	9
10.1 Authorising a Person to Access the CCTV System	9
10.1.1 Federation Council Authorised Personnel and Approved Contractors.....	9
10.1.2 Inductions.....	9
10.1.3 Issuing of Username and Passwords.....	10
10.2 Levels of Access to the System	10
10.3 Requests for the release of CCTV footage.....	10
10.3.1 Requests by the NSW Police	10
10.3.2 Requests for the emergency release of CCTV footage by NSW Police	11
10.3.3 Requests for release of CCTV footage by a Council Officer	11
10.3.4 Member of Public Request (GIPA Requests for the release of CCTV footage)	12
10.4 Federation Council Process for Retention of Images	13
10.4.1 Retention of Images	13
10.4.2 Verbal Requests for Holding of Recorded Material	13
10.5 Maintenance of System.....	13
10.5.1 Routine Maintenance.....	13
10.5.2 Monthly Maintenance.....	13
10.5.3 Camera Cleaning	14
10.6 System Failure	14
10.7 Review of and Changes to Standard Operating Procedures	14
10.7.1 Major Changes	14
10.7.2 Minor Change.....	14
10.8 System Audit.....	15
10.8.1 Internal Audit of Processes	15
11. Complaints	15
12. References & Associated Documents	16
12.1.1 References.....	16
12.1.2 Associated Documents.....	16
13. Procedure History	16
14. Reviews.....	16
APPENDIX 1 - CCTV CONFIDENTIALITY AGREEMENT	17
APPENDIX 2 - CCTV REGISTER FOR INDUCTION AND ACCESS LEVELS	18
APPENDIX 3 - INCIDENT REGISTER FORM	19
APPENDIX 4 - MONTHLY MAINTENANCE REGISTER FORM	20
APPENDIX 5 - EQUIPMENT MODIFICATION/FAILURE REGISTER.....	21
APPENDIX 6 - SYSTEM PROCEDURE CHANGE OR MODIFICATION NOTICE.....	22
APPENDIX 7 - AUDIT REPORT FORM	23

1. Purpose

The purpose of this procedure is to ensure the management and compliance of Federation Council’s installed CCTV systems and captured footage. This procedure is intended to work in conjunction with adopted CCTV Policy.

The intent of the CCTV Program is to:

- assist in reducing personal and property damage levels;
- assist Police in determining the appropriate allocation of resources in situations where the commission of a crime is imminent or is in progress;
- assist in the detection and prosecution of offenders;
- promote a safer and more liveable environment;

2. Background

Federation Council recognises the risks associated with asset management including crime is an important factor impacting its assets with concerns about safety in certain areas.

It is recognised however, that crime will never totally be prevented. CCTV cameras may bring benefits to the community, such as a reduction in crime, which can lead to enhanced community safety in a particular area. CCTV is only one of a range of strategies that Council utilises with an aim to reduce crime. Other strategies include activating public space, appropriate lighting, natural surveillance, access control and signage.

3. Scope

This Procedure provides guidance to Federation Council workers, volunteers and contractors, with respect to CCTV systems established, operated and managed by or on behalf of Council.

It does not apply to CCTV systems installed by a third party, such as a tenant or licensee of Council land and/or facilities. Although outside of the scope of this Procedure, these schemes will need approval from Council prior to installation. Council staff will consider how the proposed scheme aligns with the principles (below) prior to approving such a scheme. If approved, the scheme will be owned and operated by the organisation in accordance with appropriate legislation and guidelines.

Nor does it relate and or include mobile cameras including 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. A separate Management Policy for removable devices will be developed for this.

4. Definitions

The following definitions are for the purposes of this document:

Definition	
CCTV	A television system that transmits images within a closed system. Images are not openly transmitted but available to a specific location. The CCTV system consists of cameras, recorders, interconnecting hardware and support infrastructure, and may be fixed or portable

CCTV Programme	The implementation of a series of CCTV cameras in a public place in consultation with the NSW Police for the purposes of preventing and deterring crime at the location, particularly in response to addressing community concerns about safety.
Council Authorised Personnel	A Council employee who has been authorised by Federation Council to carry out specific tasks in the operation or management of the CCTV System
CCTV footage	means CCTV data/footage recorded by the CCTV System
Remote Access	Access to the CCTV Network via the internet
Content Manager	Federation Council's Electronic Record Management System
Public Places	Defined from the Local Government Act 1993 and refers to public reserves, public bathing reserves, public baths or swimming pools, public roads, public bridges, public wharfs or public road-ferries with the addition of public transport and car parks.
GIPA	Applications for release of images other than those made by NSW Police are to be made under the <i>Government Information (Public Access) Act 2009</i> (GIPA).

5. Responsibilities

Position	Role
Public Officer	The delegated Public Officer of Council is responsible for assisting the community with access to information, deal with community request, receive submissions and accept service of documents and other activities as defined by section 343 of the <i>Local Government Act 1993</i> . At Federation Council the delegated Public Officer is the Director Corporate & Community Services.
IT staff	IT staff are responsible for the capture, secure storage and release CCTV camera footage where release of the footage has been approved by the Public Officer, in accordance with this policy and any associated procedures.
Council staff	All Council staff (including volunteers, contractors, casual and part time employees) are required to comply with this policy and any associated procedures.
Governance Officer	Is responsible for assessing requests for release of CCTV footage under the Government Information Public Access (GIPA) Act 2009.
Director Corporate & Community Services	Is the delegated Public Officer for Federation Council and is responsible for determining requests for release of CCTV footage.
General Manager	Is responsible for ensuring this policy and any associated procedures are consistently applied.

6. Key Principles

This procedure is based on 15 Key Principles outlined in the NSW Government Policy Statement and Guidelines for the Establishment and Implementation of CCTV in Public Places:

Key Principle

1	The CCTV Program will be operated fairly, within applicable law, and only for the purposes for which it is established, or which are subsequently agreed in accordance with this standard operating procedure.
2	The CCTV Program will be operated with due regard to the privacy and civil liberties of individual members of the public, including the rights to freedom of religious and political expression and assembly.
3	The public interest in the operation of the CCTV Program will be recognised by ensuring the security and integrity of operational procedures.
4	Federation Council has primary ownership and responsibility for compliance with the purposes and objectives of the CCTV Program, for the maintenance, management and security of the CCTV Program, and the protection of the interests of the public in relation to the Program.
5	As a partner to Federation Council CCTV Program, the NSW Police Force will act in accordance with this standard operating procedure.
6	Federation Council will be accountable to the public for the effective operation and management of the CCTV Program.
7	The public will be provided with clear and easily accessible information in relation to the operation of Federation Council's CCTV Program.
8	Regular monitoring and evaluation of the CCTV Program will be undertaken to identify whether the purposes of the Program are being complied with and objectives are being achieved.
9	Staff with access to a CCTV control room, whether they be operators or managers, will meet the highest standards of probity.
10	Access to the CCTV footage and any control room will be restricted to authorised staff and their managers as stated in the SOP and a control room and its data will be protected from unauthorised access.
11	Information recorded will be relevant and not exceed that necessary to fulfil the purposes of the CCTV Program.
12	Information will be obtained fairly and in accordance with the privacy provisions of this standard operating procedure.
13	The retention of, and access to photographs and recorded material will be only for the purposes provided by this standard operating procedure. CCTV data will be retained for up to 30 days unless they are required in relation to the investigation of crime or for court proceedings. Recorded material no longer required will be disposed of using approved methods.
14	Contact related to the CCTV Program between Federation Council's staff and the Police, will be conducted strictly in accordance with this standard operating procedure.
15	The CCTV Program must address the interests of all who may be affected by it, and not be confined to the interests of Federation Council or the needs of the criminal justice system.

7. Risk Management

Federation Council with its vast risk profile, and limited resources, understands the need to minimise loss, and maximise opportunities, this ensuring long term sustainability. Council's risk management framework 17/34556 and processes are in accordance with AS/NZS ISO 31000:2020 – Risk Management – Principles and Guidelines and HB 436:2013 – Risk Management Guidelines, provides an adopted process to identify, analyse and control risks that may adversely impact objectives.

The objective of the risk management process is to ensure that:

- All significant operational and organisational risks are understood and identified
- The highest risks that need to be addressed in the short to medium term are identified
- Strategies and treatments to address risks are identified and applied

An assessment risks identified, via a number of sources including:

- Inspections
- Reports and complaints from general public
- Information obtained from incidents
- Knowledge and past experience

The risk assessment process identifies and assesses risks, develops a risk rating and develops a risk treatment plan for non-acceptable risks.

Risk ratings are determined using Federation Councils risk matrix:

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Moderate 8	High 16	High 20	Extreme 23	Extreme 25
Likely	Moderate 7	Moderate 12	High 17	High 21	Extreme 24
Possible	Low 4	Moderate 10	High 15	High 18	High 22
Unlikely	Low 2	Low 5	Moderate 11	Moderate 13	High 19
Rare	Low 1	Low 3	Moderate 6	Moderate 9	High 14

Key risk management criteria relating to Council’s CCTV programme include:

- Environmental and legal compliance
- Financial
- Property and Infrastructure
- Public Liability
- Reputation

8. System Description, Locations & Purposes

Under Federation Council’s CCTV Program, CCTV systems have been installed primarily for the purposes of security and risk management including protection of council’s assets from vandalism. CCTV systems operate on a continuous 24-hour basis.

In some situations, installation of CCTV enables Federation Council and the NSW Police to work together to help provide a safer environment, reduce crime levels by deterring potential offenders, aid crime detection and the apprehension of offenders.

It is acknowledged that CCTV systems installed in public place locations and as part of the Federation Council assets may also capture council staff performing work tasks. CCTV systems subject to this Program are not designed to intentionally provide workplace surveillance. A separate Management Policy will be developed for this.

When installing CCTV systems, Federation Council will ensure:

Federation Council - Closed Circuit Television (CCTV) Standard Operating Procedure

15/11/2024 5:12 PM

Reference: 21/44752

Version No: 1

Page 7

- Clearly visible signs that CCTV are operating will be displayed at the perimeter of the area covered by the system and at other key points.
- The locations of CCTV cameras will be clearly apparent to the public.
- CCTV cameras will not be used to look into adjacent or nearby premises or buildings. Any misuse is to be treated as a breach of this procedure and subject to disciplinary action.
- No sound will be recorded in public places.
- 'Dummy' CCTV cameras will not be used.
- CCTV data will not be sold or used for commercial purposes or the provision of entertainment
- Appropriate security measures will be taken against unauthorised access to, alteration, disclosure, accidental loss or destruction of recorded material

CCTV systems have been installed in the following locations, for the purposes (listed below):

Site	Location	Camera Type	Purpose(s)
Corowa Civic Centre including the Corowa Library and Visitor Information Centre	100 Edward Street Corowa	Fixed	<ul style="list-style-type: none"> • Security • Risk Management • Crime prevention
Corowa Aquatic Centre	100 Edward Street Corowa	Fixed	<ul style="list-style-type: none"> • Security • Risk management • Crime prevention
Corowa Plaza Sanger Street	Sanger Street Corowa	Fixed	<ul style="list-style-type: none"> • Security • Crime Prevention
Howlong Library	59 Hawkins Street Howlong	Fixed	<ul style="list-style-type: none"> • Security • Risk Management
Mulwala Library	71 Melbourne Street Mulwala	Fixed	<ul style="list-style-type: none"> • Security • Risk Management
Corowa Council Depot	24 Poseidon Road Corowa	Fixed	<ul style="list-style-type: none"> • Security • Risk Management
Urana Depot	Frederick Street Urana	Fixed	<ul style="list-style-type: none"> • Security • Risk Management
Oaklands War Memorial Swimming Pool	3 Hunter Street Oaklands	Fixed	<ul style="list-style-type: none"> • Security • Risk Management • Remote supervision
Urana War Memorial Swimming Pool	Federation Way Urana	Fixed	<ul style="list-style-type: none"> • Security • Risk Management • Remote supervision
Construction sites	Identified as part of the project management brief.	Temporary	<ul style="list-style-type: none"> • Security • Monitor construction progress – time in motion studies

9. New CCTV Systems

Any installation of new CCTV systems should be done taking into account those key principles outlined in Federation Council's CCTV Policy. Where a CCTV scheme is proposed for a public space for crime prevention or community safety, it should be considered in consultation with NSW Police Force Murray River District. Approval from the Executive Management Team (Manex) must be obtained prior to proceeding with a CCTV scheme for crime prevention purposes.

CCTV systems installed by Federation Council should meet the following requirements:

- It must be either a Hikvision or Ubiquiti brand camera system. These two brands achieve simplicity in management, but also provide broad capability and prevent vendor lock-in.
- It must be capable of storing a minimum of 30 days of footage from all attached cameras.
- It must use infrared-lit night-vision cameras.
- It must use cameras of at least 1080p resolution.

- It must have multiple IP Network interfaces on the video record unit to allow for one to be used for the Camera IP Network, one to be used for management connection to the wider council network. This is to segregate the cameras from the corporate data network to prevent unauthorised access to camera feeds.

It is the intention that all CCTV systems are interfaced with Council's network system enabling the IT Department ability to securely manage and access remotely.

Council staff must liaise with the IT Department prior to purchase or installation of any new CCTV systems or modification or replacement of existing CCTV systems. Any new installation or upgrade projects must consider whether there is sufficient network infrastructure in place to support a new connection with consultation with council's IT Department. Stand-alone CCTV systems are not encouraged or supported. The only exception are temporary CCTV systems used at construction sites for time in motion studies.

10. Standard Operating Procedures

This Standard Operating Procedure outlines how the operation of Federation Council's CCTV System will be managed. This Standard Operating Procedure should be read in conjunction with the CCTV Policy. Federation Council Authorised Personnel must understand and comply with the contents of these Standard Operating Procedures. Any modifications to these Standard Operating Procedures must be consistent with the CCTV Policy.

10.1 Authorising a Person to Access the CCTV System

10.1.1 Federation Council Authorised Personnel and Approved Contractors

Authorised council personnel and approved contractors must:

- understand their responsibilities for maintaining privacy;
- comply with these procedures; and
- be competent in operating or maintaining the system.

10.1.2 Inductions

Identified authorised council personnel and approved contractors must complete a CCTV Induction. Inductions will be carried out by the Manager IT & Customer Service or their delegate. The following documents will be supplied and explained to the inductee by the inductor:

- a) Council's CCTV Policy;
- b) Council's CCTV Standard Operating Procedures;
- c) Council's Code of Conduct; and
- d) Council's Privacy Policy.

Contractors must complete and supply Council with the following prior to being approved to undertake any works on council's CCTV systems:

1. Confirmation of completed Council's online contractor induction
<https://www.linksafe.com.au/federationcouncil>
2. A copy of the required NSW Security Licence (if they are working on the system)

At the completion of the induction, council authorised personnel and approved contractors must sign a Confidentiality Agreement (21/44716) to the effect that they have read, understood and agree to abide by the CCTV Policy (21/44751) and this Standard Operating Procedures (21/44752).

On the completion of the induction, the inductee shall be approved by the Manager IT & Customer Service and their induction shall be recorded in the Register of Induction and Authorised Persons (21/44717).

10.1.3 Issuing of Username and Passwords

A Federation Council authorised employee or approved contractor who requires access to the CCTV system, as a part of their duties, will be issued a unique username and an initial password by the Manager IT & Customer Service or the IT Systems Administrator. The user is responsible for actions and use under the user’s logon. Approved contractors will be issued temporary access to undertake approved work. This access will be revoked when they have completed the works.

10.2 Levels of Access to the System

The following are designated levels of access for the system.

Level	Purpose	Who
Level 1	Camera viewing and reviewing	<ul style="list-style-type: none"> • Directors • Authorised Managers/Coordinators • Duty Officer Pools • Risk Management Coordinator (for reported incidents, insurance and public liability matters only) • Governance Officer (for GIPA requests only)
Level 2	Camera viewing and reviewing Recording still images for approved export Redacting information on footage (authorised under GIPA assessments)	<ul style="list-style-type: none"> • IT Systems Administrator • IT Support Officer
Level 3	Full access for system administration Maintenance and approved modifications (temporary for approved works only)	<ul style="list-style-type: none"> • Manager IT & Customer Service • IT Systems Administrator • Approved contractors

10.3 Requests for the release of CCTV footage

10.3.1 Requests by the NSW Police

Release of images to NSW Police must be in accordance with the CCTV Policy and this procedure.

To request the release of CCTV footage, the NSW Police must:

- Send a request to Council’s email at: council@federationcouncil.nsw.gov.au
- The request should identify the time, location and description of the recorded material required.
- The request should identify the name of the Police Officer and come from an official NSW Police email account.
- On receipt of the request:
 - Records will register the request in Content Manager Container SC6132 and record the incident(s) on Council’s Incident Register (21/44718).
 - The request will then be sent to the Manager IT & Customer Service to initially determine if the requested CCTV footage is within the 30-day timeframe. If the requested CCTV footage is within the required 30-day timeframe the Manager IT & Customer Service will immediately arrange for the requested CCTV footage to be exported into a short-term secure storage area.

- The Manager IT & Customer Service will then update the Incident Register (21/44718) and place a note on the request advising that the CCTV footage has been exported, and its location.
- The request should then be sent to the Director Corporate & Community Services for approval.
- The Director Corporate & Community Services, will determine the request and make a note on request advising if the requested CCTV footage is approved/not approved for release to the NSW Police.
- If the CCTV footage has been approved for release, then the CCTV footage should be emailed to the applicant via council's secure Online File Transfer. The file is uploaded to Federation Council's server with password access and if required the capability to only allow one download.
- If the CCTV footage has been released, IT will receive a receipt advising that the footage has been received, the time the footage has been download and location. The Manager IT & Customer Service will record the receipt number and time of download on the Incident Register form (21/44718). The CCTV footage should be retained in the short-term secure storage area for a 90-day period.
- If the CCTV footage request has not been approved the Manager IT & Customer Service will advise the Police Officer and place a note on the request advising that the request was not approved.
- It should be noted that Federation Council has no control over what happens after the file is downloaded.
 - The NSW Police force may at times request an affidavit. These requests are required to be registered into Content Manager Container SC6132, related to the original request and work flowed to the Director Corporate & Community Services for signature.

10.3.2 Requests for the emergency release of CCTV footage by NSW Police

In exceptional circumstances, emergency access to CCTV footage may be required by the NSW Police outside of normal business hours. In these circumstances, NSW Police should contact either council's General Manager who will then contact the Manager IT & Customer Service to arrange access to CCTV footage.

10.3.3 Requests for release of CCTV footage by a Council Officer

- Council Officers are required to report all incidents of vandalism or damage to council property or assets using council's Incident Report Form (18/25348), including an estimated value of damage
- Vandalism incident guidelines are as follows:
 1. \$0 - \$100 - minor maintenance repairs should be undertaken, and no Police Report is required.
 2. \$100 - \$1000 - An online Police Report is required to be entered via <https://portal.police.nsw.gov.au> and a Police Report Number will be generated.
 3. \$1000 – or more – It is required to attend the Police Station to report the incident and obtain a Police Report Number.
- A completed Incident Report Form is to be signed off via manager/director and then sent to council's Risk Management Coordinator.
- On receipt of completed form the Risk Management Coordinator will assess the Incident Report and determine if CCTV footage is within the required 30-day period and the value of the damage. If the Risk Management Coordinator determines that CCTV footage is required the Risk Management Coordinator will send a request to the Manager IT & Customer Service to extract CCTV footage. The request should identify:
 1. Time;
 2. Date;
 3. Location;
 4. A brief description of the recorded material required.
 - I. On receipt of the request the Manager IT & Customer Service will record the incident(s) on Council's Incident Register (21/44718).
 - II. The Manager IT & Customer Service will immediately arrange for the CCTV footage to be exported into a short-term secure storage area. The Manager IT & Customer Service will then update the Incident Register with the location and date the data has been exported.
 - III. The Risk Management Coordinator will review the footage and determine if it is required to be released to any third parties for insurance or liability reasons. If after viewing the footage the Risk Management

- Coordinator believes the footage is required to be released to third parties, they will send the this request to the Director Corporate & Community Services for their approval.
- IV. The Director Corporate & Community Services, will determine the request and make a note on request advising that the requested CCTV footage is approved/not approved for release to third parties.
 - V. If approved, the Manager IT & Customer Service will action the release of the CCTV footage by emailing to the third party via council's secure Online File Transfer. The File is uploaded to Federation Council's server with password access and if required the capability to only allow one download. IT will receive an email receipt advising that the email has been received, the time the footage has been download and location. The receipt number and time of download should be recorded on the Incident Register form (21/44718). The CCTV footage should be retained in the short-term secure storage area for a 90-day period.
 - VI. If the request has been denied, then the Risk Management Coordinator should be advised that the footage has not been approved for release. The Director Corporate & Community Services will place a note on the request advising that the request has been refused including the reason.
 - VII. The Manager IT & Customer Service will update the Incident Register.

10.3.4 Member of Public Request (GIPA Requests for the release of CCTV footage)

Applications for release of images other than those made by NSW Police are to be made under the *Government Information (Public Access) Act 2009* (GIPA). A member of the public has the right to apply for access to personal information held by Federation Council in the following ways:

A person can apply for information under the *Government Information (Public Access) Act 2009*. A copy of the Government Information (Public Access) Act 2009 - Formal Access Application Form can be obtained from Federation Council's website www.federationcouncil.nsw.gov.au, standard GIPA application fees will apply.

Federation Council's Governance Officer will make a determination of the validity of applications and may request a viewing of relevant images to assist in their determination.

Determination of the validity of a request must consider the following:

- a) Whether the form has been signed and contains all relevant information;
- b) Whether the date of the incident is within 30 days of the application being submitted or the relevant images have already been saved to a secure short term storage;
- c) Whether the location has CCTV cameras in operation;
- d) Whether the application contains sufficient details of the incident(s) to identify the relevant recorded images;
- e) Whether the release of the images would breach any legislative or statutory requirement of Council;
- f) Whether the images impact on the privacy of other people in the images;
- g) Whether the images relevant to the GIPA application?

Applications can be rejected for the following reasons:

- a) The incident listed does not fall within 30-day period;
- b) The application is not signed;
- c) The incident did not occur within the areas under surveillance;
- d) The application is a duplicate of an application already received;
- e) The CCTV footage relating to the incident is corrupted;
- f) Releasing the images impact on the privacy of other people in the images;
- g) Releasing of the images would breach any legislative or statutory requirement of Council;
- h) There is no incident or relevant images relating to the incident or request.

On receipt of a GIPA application:

- The Governance Office will ensure payment has been received and then commence the GIPA assessment.
- If the requested CCTV footage is within the required 30-day timeframe. The application form should be sent to the Manager IT & Customer Service to immediately arrange for the requested CCTV footage to

be exported to a short term secure storage area and record the incident on Federation Council's Incident Register (21/44718).

- The Manager IT & Customer Service will then update the Incident Register (21/44718) and place a note on the request advising that the CCTV footage has been exported, and its location.
- The Director Corporate & Community Services, will determine the request and make a note on request advising that the requested CCTV footage is approved/not approved for release of the CCTV footage as part of the GIPA application.
- If approved, the Manager IT & Customer Service will action the release of the CCTV footage by emailing to the GIPA applicant via council's secure Online File Transfer. The File is uploaded to Federation Council's server with password access and if required the capability to only allow one download. IT will receive an email receipt advising that the email has been received, the time the footage has been download and location. The receipt number and time of download should be recorded on the Incident Register form (21/44718). The CCTV footage should be retained in the short-term secure storage area for a 90-day period.
- If the request has been denied, then the Governance Officer should be advised that the footage has not been approved for release. The Director Corporate & Community Services will place a note on the request advising that the request has been refused including the reason.
- The Manager IT & Customer Service will update the Incident Register.
- It should be noted that Federation Council have no control over what happens after the file is downloaded or if it is copied.

10.4 Federation Council Process for Retention of Images

10.4.1 Retention of Images

All CCTV footage will be retained for a minimum 30 days unless it is the subject of an application. All recorded material on the CCTV System shall be overwritten on a 30-day cycle.

All CCTV footage that has been quarantined into the short term secure storage area will be disposed of after 90 days.

10.4.2 Verbal Requests for Holding of Recorded Material

Under exceptional circumstances, where images may be in danger of expiring, or a Council Officer has reported an incident a verbal request for the holding of CCTV footage may be made. These requests should be made to the Director Corporate & Community Services. After approval from the Director Corporate & Community Services, the Manager IT & Customer Service will ensure that the relevant CCTV footage is copied to a secure short-term secure storage area. This CCTV footage may only be used or released should the Director Corporate & Community Services approve a request for the supply of a copy of CCTV footage. If no written application is received within 90 days, the Manager IT & Customer Service will ensure the images are deleted from the short-term secure storage.

10.5 Maintenance of System

10.5.1 Routine Maintenance

The following procedures shall be carried out as a part of "due diligence" to ensure the cameras are operating to specifications.

10.5.2 Monthly Maintenance

Monthly maintenance checks will be performed by Council's IT team.

The Manager IT & Customer Service will ensure a thorough monthly check is performed on the fourth day each month which will include:

- a) An “Equipment Modification Failure Report” (Appendix 5) to identify any outages in previous month on the system;
- b) Check recording time on the archive;
- c) Check recording are working by playing back segments of the footage and review notifications;
- d) Check time synchronisation is updated and working. These checks are to be recorded on the Monthly Maintenance Register form (Appendix 4), by the Council Authorised Personnel carrying out the check;
- e) Check footage can be seen from all cameras and the camera positions are correct.

10.5.3 Camera Cleaning

The council’s Facility Management team will organise for cameras to be cleaned on an as needed basis, where issues have been identified.

10.6 System Failure

Incidents of failure should be reported to council’s IT team.

The Manager IT & Customer Service will ensure each system failure or equipment failure shall be logged and recorded in the Equipment Modification/Failure Register (Appendix 5). On identification of a failure, the Manager IT & Customer Service will carry out standard diagnostic procedures to identify and rectify the problem. If needed, the Manager IT & Customer Service will work with the Facility Management team to organise for the problem to be fixed.

10.7 Review of and Changes to Standard Operating Procedures

These Standard Operating Procedures are subject to review in conjunction with the review of the CCTV Policy. When an approved change is made, both documents require the quality control table to be updated.

10.7.1 Major Changes

A major change to this Standard Operating Procedures can only be made after consultation with the NSW Police Force and upon agreement of Federation Council. Major changes must consider any requirements of the CCTV Policy.

A major change is any change that will have significant impact upon the implementation of the CCTV Policy. An example of a major change is a change to the purpose of the system or proposal to install further permanent cameras.

Any major change to the Standard Operating Procedures will be included in the evaluation report.

10.7.2 Minor Change

A minor change to this Standard Operating Procedures may be made with the agreement of the General Manager.

A minor change is a change to the existing document that does not affect the meaning or intent of this Standard Operating Procedure.

Amendments that are minor in nature include, but are not limited to, the following:

- Changes to the format;
- Changes to the title or name of a position, Directorate, Group, Team, document, publication, address (including URL), or legislation referred to in the existing document;
- Correcting spelling or grammar;
- Editing for language consistency; and/or
- Change to those responsible for implementing the document as a result of an organisational restructure.

10.8 System Audit

10.8.1 Internal Audit of Processes

A random process internal audit shall be carried by out on a quarterly basis by the Records team.

The audit shall:

- Consist of selecting two random requests which have required export of images;
- Check each part of the process and documentation is consistent with the Standard Operating Procedures;
- Include a comparison to the electronic system records and the Content Manager recorded documents; and
- Check that CCTV footage temporarily stored in the short term secure storage area is disposed of after 90 days.

The results of the audit shall be recorded on the Audit Report Form (21/44719) by the Records team.

On a quarterly basis, the IT team will:

- Check the System Equipment Failure Log for:
 - Regular failures
 - Rectification response times.

11. Complaints

Council has a complaint handling procedure and process and this will be provided on request.

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

The General Manager Federation Council
100 Edward Street,
COROWA NSW 2646

The General Manager will inform the Director of Corporate and Community Services of each complaint received, and how it was dealt with.

- Where a complaint cannot be resolved within Council, the complainant will be referred to an outside agency to seek resolution.
- Section 36 of the Privacy and Personal Information Protection Act 1998 authorises the Privacy Commissioner to receive and investigate complaints about alleged violations of privacy. Any member of the public is entitled to lodge a complaint with the Privacy Commissioner.
- Council will cooperate with the investigation of any complaint by the Privacy Commissioner.

The Privacy Commissioner can be contacted at:

Information and Privacy Commission
NSW GPO Box 7011
SYDNEY NSW 2001
Telephone 1800 472 679
Email ipcinfo@ipc.nsw.gov.au

12. References & Associated Documents

12.1.1 References

Council, in developing this procedure, referred to the following public documents:

- NSW Government policy statement and guidelines for the establishment and implementation of closed circuit television (CCTV) in public places http://www.crimeprevention.nsw.gov.au/Documents/Councils-Publications/CCTV_guidelines.pdf
- New South Wales Police Force <https://portal.police.nsw.gov.au>
- AS/NZS 62676.1.1:2020 - System Requirements
- <https://www.ipc.nsw.gov.au/fact-sheet-managing-access-audio-visual-information-under-gipa-act>
- <https://www.privacy.org.au/Resources/PLawsST.html>
- Broken Hill City Council CCTV standard Operating Procedure
- Wollongong City Council CCTV Code of Practice
- Lake Macquarie City Council CCTV Policy
- NSW Privacy and Personal Information Protection Act 1988.
- NSW Workplace Surveillance Act 2005.
- NSW Government Information (Public Access) Act 2009.
- NSW Surveillance Devices Act 2007

12.1.2 Associated Documents

Council's CCTV Policy (21/44751)

Forms and registers form part of these procedures:

- Appendix 1 - Confidentiality Agreement (21/44716)
- Appendix 2 – CCTV Register for Induction and Access Levels - (21/44717)
- Appendix 3 - Incident Register Form (21/44718)
- Appendix 4 – Monthly Maintenance Register Form (21/44714)
- Appendix 5 – Equipment Modification/Failure Register (21/44715)
- Appendix 6 - System/procedure Change or Modification Notice (21/44720)
- Appendix 7 – Audit Report (21/44719)

13. Procedure History

Version	Date	Changes / Amendments
1	16 August 2020	Initial Draft Adopted at the February 2023 Council Meeting

14. Reviews

This standard operating procedure will be review and updated accordingly every two (2) years.

NOTE: This is a controlled document. If you are reading a printed copy please check that you have the latest version by checking it on Councils Electronic Document system. Printed or downloaded versions of this document are uncontrolled.

APPENDIX 1 - CCTV CONFIDENTIALITY AGREEMENT



CM No. 21/44716

I, an employee of
Federation Council

Agree to:

- 1. Not disclose, unless lawfully directed, any matter or information which comes to my knowledge in relation to or emanating from the operation of the Public CCTV System operated by Federation Council;
- 2. Not use the contents of the CCTV footage:
 - 2.1. To gain advantage for me or for any other person or body;
 - 2.2. To improperly cause harm or detriment to any person, body, or Federation Council.
- 3. Further agree to:
 - 3.1. Protect information relating to the operation of the Federation Council CCTV System, including the CCTV footage;
 - 3.2. Not disclose any information discussed during a meeting with Federation Council staff regarding the CCTV footage;
 - 3.3. Maintain the integrity and security of the CCTV footage and relevant information;
 - 3.4. Comply with Federation Council’s Privacy Management Plan when dealing with personal information as well as the provisions of the *Privacy and Personal Information Protection Act 1998*, Information Protection Principles and the Privacy Policy for Local Government and other relevant privacy or surveillance legislation;
 - 3.5. Abide by Federation Council’s Code of Conduct, CCTV Policy, CCTV Standard Operating Procedure and Workplace Surveillance Policy;
 - 3.6. Not to reproduce CCTV footage in any manner or way for any purposes, unless authorised by Federation Council to do so.

Signed: _____

Signature of Witness: _____

Name: _____

Name of Witness: _____

Date: _____

APPENDIX 4 - MONTHLY MAINTENANCE REGISTER FORM

Monday - Friday

PO Box 100

COROWA NSW 2646

council@federationcouncil.nsw.gov.au
www.federationcouncil.nsw.gov.au

CM No. 21/44714

General Enquiries

Phone: 02 6033 8999

Performed by:

Date:

Equipment Failure Report run?	Yes	No
Recording time on archive is correct?	Yes	No
Time synchronisation accurate?	Yes	No
Play back	Yes	No
Camera position correct?	Yes	No
Check images are clear	Yes	No
Any issues identified?	Yes	No

Action taken:

Do any of the issues require recording in the Equipment Failure Register?	Yes	No
Details of issues and actions recorded in the Equipment Failure Register	Yes	No

APPENDIX 6 - SYSTEM PROCEDURE CHANGE OR MODIFICATION NOTICE

CM No. 21/44720

Date of notification _____

Alteration/Incident No _____

System Description _____

Location of Alteration _____

Reason for Alteration _____

Type of Alteration _____

Does the alteration modify any or the system parameters? If yes,
please provide detail _____

Are the camera views modified? _____

Is the current coverage affected? _____

Are there System modification or changes required? _____

Are CCTV Operations modified? _____

DETAILS OF MODIFICATIONS

Does the alteration/s Conform with the CCTV Policy and
Standard Operating Procedure _____

Is Public Consultation and/or notification required? _____

Document prepared by: _____

Authorised by: _____

APPENDIX 7 - AUDIT REPORT FORM

CM No. 21/44719

General Enquiries

Phone: 02 6033 8999

SECTION 1 – INTERNAL AUDIT

Date:

Auditor:

Documents Audited

I confirm these documents conform to the requirements of the Council CCTV Policy and Standard Operating Procedures.

Yes

No

If No, please attach relevant documentation noting discrepancies

Signed:

Date: