1.0 PURPOSE

This procedure provides a framework for the installation, operation and management of Council's CCTV surveillance system network and the management of any associated data in accordance with relevant legislation.

2.0 SCOPE

This procedure applies to fixed and mobile CCTV camera infrastructure and systems installed at any Council owned or managed location within its jurisdiction and is applicable to all Council officers, Councillors and any other parties involved with installation, management and maintenance of Council's CCTV cameras.

The overall standards which Council's CCTV network will be operated are based on the following principles:

- In partnership with law enforcement agencies, Council aides in crime prevention and promotes community safety whereby CCTV will be utilised for the protection of Council's resources encompassing both physical assets and people;
- CCTV footage may be utilised to assist law enforcement agencies in the investigation of reported crimes or incidents;
- Council will assess all CCTV placement requests in accordance with the CCTV installation request process outlined in this procedure;
- CCTV equipment specifications will be suitable to achieve the purpose intended and positioned in a secure manner that does not intrude to a reasonable extent on an individual's privacy;
- The system will be secure and footage accessed only by authorised officers;
- CCTV systems will be operated, maintained and accessed in accordance with the IP Act and *Invasion of Privacy Act 1971;*
- Extracted footage will be stored in accordance with the *Public Records Act 2002*.

3.0 DEFINITIONS/ABBREVIATIONS

CCTV	Closed-circuit television is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors.
Collection Notice	Formal public notice used to inform individuals why their personal information is being collected, if a law requires the collection and what the information will be used for including any potential disclosure to third parties.
MOU	Memorandum of Understanding
IP Act	Information Privacy Act 2009 (Qld)
Officer	Employee, contractor or volunteer engaged by Bundaberg Regional Council
QPS	Queensland Police Service
RTI Act	Right to Information Act 2009 (Qld)

4.0 RESPONSIBILITY AND/OR AUTHORITIES

4.1 Information Services: ownership and ongoing responsibility for resourcing, installing, maintaining and repairing Council's CCTV systems and associated equipment.

Governance & Legal Services: responsible for governing the operations of the camera network and managing processes to capture, secure, use and disclose data in accordance with relevant legislation.

Venues & Facilities: responsible for establishing the need for CCTV monitoring in council facilities and assets, reporting known outages and contract management of security service providers.

Office of the CEO: responsible for the approval of new camera network placements and/or additional cameras on existing networks.

5.0 REFERENCES/ASSOCIATED DOCUMENTS

Information Privacy Act 2009

Invasion of Privacy Act 1971

Right to Information Act 2009

Public Records Act 2002

CP-3-037 Recordkeeping Policy

FM-7-1088 CCTV Information Request - Internal Use

FM-7-1089 Personal Information Request - External Agencies

FM-7-1128 Queensland Police Service (QPS) Personal Information Request

MD-7-587 Naming Convention Standard and Guidelines

OP-3-135 Electronic Surveillance Policy

6.0 DOCUMENT ENQUIRIES

Position Title: Governance Officer

7.0 PROCEDURE

7.1 CCTV INFRASTRUCTURE

7.1.1 All cameras will be positioned in a way to capture the designated surveillance area and not unreasonably intrude on an individual's privacy or neighbouring properties.

7.1.2 No cameras or surveillance equipment are to be placed in or be positioned in a manner to record people in any place that one would reasonably expect privacy such as bathrooms or change rooms.

7.1.3 Damage to any CCTV cameras or equipment is to be reported as soon as practical to the Information Services team, via the lodgement of a IT helpdesk request.

7.1.4 Access to CCTV controls and recorders shall be limited only to authorised officers and secured via unique login and password credentials.

7.1.5 Where possible CCTV networks will be connected to an uninterrupted power supply to ensure best efforts towards business continuity in the event of loss of power supply.

7.1.6 All new CCTV requests will undergo an evidence-based decision-making process to determine suitability for installation as outlined in CCTV installation process below.

7.1.7 CCTV systems will be configured to ensure captured footage is retained for a period of 30 days after which the system will automatically overwrite footage.

7.1.8 CCTV infrastructure and systems may be installed in premises under leasing arrangements by the lessee, subject to the terms outlined in the lease agreement.

7.2 CCTV INSTALLATION

7.2.1 Requests for CCTV installation will require the following supporting documentation:

7.2.1.1 Completion of the CCTV Camera Installation, Repair & Access Request form submitted to the Governance Officer addressing the following criteria:

- a clear purpose to determine appropriateness of the installation of a CCTV system outlining what the system will be used for;
- evidence or reasoning demonstrating how the use of camera surveillance will achieve the purpose;
- the proposed positioning of the cameras and span of the surveillance area demonstrating placement that will effectively capture only the intended surveillance area;
- proposed systems access controls documenting any person/s requiring access and the level of access required;
- identification of costs including equipment purchase, installation and ongoing maintenance costs.

7.2.2 Request for CEO approval will be submitted by Governance Officer upon review of the above listed information.

7.2.3 If the request is approved all affected parties will be notified of the decision and the applicant is to liaise with Information Services to begin scheduling of works.

7.2.4 If a request has not been supported, the applicant will be notified and provided with reasons for same.

7.3 SIGNAGE

7.3.1 All areas subject to CCTV monitoring must be signed appropriately to advise anyone entering the surveillance area, they may be recorded.

7.3.2 Any signage displayed will comply with requirements outlined in Information Privacy Principle 2 of the IP Act. Signage is available from the Information Services team and the following requirements will be applicable:

- fixed signs will be placed at each main access point to any surveillance area;
- signs are made of a weatherproof material and contain a collection notice;
- signs are branded with Council's logo and prepared with the intention to be clearly visible, distinctive and located in areas with good lighting, and placed within normal eye range;
- signs will be checked regularly for damage and theft and replaced where required;
- in situations where signage is not practical, Council officers must be able to communicate with any affected parties the purpose use and disclosure of any information captured.

7.3.3 Where electronic surveillance is no longer occurring, all signage and equipment will be removed as soon as practical.

7.3.4 Signage is not permitted to be erected in areas where cameras are not present or likely to be present.

7.4 AGREEMENTS

7.4.1 Council will work in collaboration with law enforcement agencies with respect to the disclosure of footage for law enforcement purposes.

7.4.2 Any such arrangements entered into with contractors, or other agencies may be documented in a formal Memorandum of Understanding (MOU) or agreement.

7.4.3 Any service arrangement entered into with a non-Queensland Government agency that involves collection or management of personal information will require Council to bind the entity to the privacy principles under the IP Act as required.

7.4.4 QPS Arrangement

7.4.4.1 Council will provide an operating system to the QPS Bundaberg and Childers station designed to provide "view-only" access to nominated cameras and requested archived footage in Council's CCTV network.

7.4.4.2 QPS may request "view-only" access to additional cameras with the provision of a written request to the Governance Officer documenting the business requirement for the access.

7.4.4.3 If footage is to be extracted for the purposes of an official law enforcement investigation, QPS personnel must lodge a completed Queensland Police Service (QPS) Personal Information Request form detailing footage requirements.

7.4.4.4 Council's Governance & Legal Services team will assess the request to determine if disclosure is permissible under the IP Act. Upon approval, the footage and completed Evidence Admissibility Certificate required under section 95 of the *Evidence Act 1977* will be provided to QPS. A copy of same, including approval documentation will be retained by Council.

7.5 SECURITY & CONTROLS

7.5.1 All Council access to the CCTV network and footage contained within will be restricted to nominated authorised officers and not viewed or extracted without official cause.

7.5.2 Council maintains ownership of all physical assets associated with the CCTV network regardless of the location of the infrastructure and reserve the right to access this equipment for the purposes of maintenance or removal at Council's discretion.

7.5.3 CCTV controls and records are stored on a secure server in a restricted access facility to protect any personal information against unauthorised access, use or modification.

7.6 CCTV FOOTAGE

7.6.1 Council's CCTV network will only be actively monitored in real time by QPS unless monitoring by Council officers is required for the early identification and rapid response to anti-social behaviours for identified law enforcement operations.

7.6.2 Council officers will ensure extracted footage is captured and accurate metadata is recorded against the file (including date and time), ensuring it is stored accurately and accessible where required.

7.6.3 Council officers will only use personal information in accordance with obligations in the privacy principles outlined in the IP Act.

7.6.4 Footage containing personal information will be stored securely using unique login and password credentials in corporate systems designed to prevent loss, unauthorised access, use or modification.

7.6.5 Requests for CCTV footage

7.6.5.1

- **External persons** - Right to Information/Information Privacy Access Application submitted to Council, with payment of the relevant fee (if applicable).
- **QPS** - QPS Personal Information Request Form.
- **Government agency** - External Agency Personal Information Request form or via a Right to Information Access Application for footage that cannot be released under any other legislative process or lawful means.
- **Internal Council officers** - CCTV Information Request - Internal Use form.

7.6.6 Any CCTV footage captured on Councils CCTV network will be retained for a period of 30 days after which, footage will be overwritten and consequently destroyed except for copies of extracted footage which is stored in accordance with Council's Recordkeeping Policy.

7.6.7 CCTV footage will only be extracted upon the receipt of a written application for personal information, as referenced above in section 7.6.5.

8.0 RECORDS

Footage extracted from the CCTV network is a public record and as such, officers need to consider their recordkeeping obligations. All requests for CCTV footage and the associated extracted footage is to be stored in a recordkeeping system using unique login and password credentials in accordance with Council's Recordkeeping Policy and the following instructions:

1) extract the required footage in an easily accessible format;
2) upload the extracted files to Councils SharePoint site;
3) ensure the appropriate metadata is recorded against the file according to the subject matter captured and apply any appropriate security controls;
4) open the file and check that it can be viewed in its entirety and has not been corrupted during the transfer process.

All requests and approvals for footage received at Council are to be recorded in Objective where the appropriate metadata and security controls will be applied, and access is restricted using unique login and password credentials.