CCTV POLICY

CATEGORY:	Engineering	**STATUS:**	Draft
DATE POLICY ADOPTED:	16 October 2018	**APPROVAL BY:**	Council
REVIEW PERIOD:	3 years	**NEXT REVIEW DUE BY:**	2021
DATE PREVIOUSLY ADOPTED:	February 2015	**REVISION NUMBER:**	1

RATIONALE

The Council's aim through the installation of CCTV (Closed Circuit Television System) is:

- to improve safety for staff, our contractors and the public;
- to deter potential vandalism and damage;
- to assist in council by-law enforcement;
- to assist in enhancing the operational effectiveness and safety of Council facilities and services; and,
- to use, where appropriate, for law enforcement purposes.

This policy applies to the on-going use of the systems (cameras, recording and viewing equipment) and data, whether on site or elsewhere, to ensure compliance with the Privacy Act 1993 (the Act) and other legislation. It is important that the system design, use and management complies with relevant sections of the Privacy Act and that recorded data is managed diligently. Compliance with the Act is necessary as CCTV data may include information covered by that Act.

PURPOSES OF POLICY

1. To ensure the Council, its employees and contractors comply with good practise, transparency and accountability including the relevant requirements of the Privacy Act.
2. To protect the privacy rights of the Council, its employees, contractors and the public.
3. To manage access to CCTV and its recorded data.
4. To ensure any required recorded data is not compromised and can if necessary be used in court as evidence.

APPLICATION OF POLICY

This policy applies to CCTV systems or cameras; which are owned or operated by or on behalf of the Council. The application of the policy is subject to the provisions of the Privacy Act, The Local Government Official Information Act, and other relevant legislation.

NON-COUNCIL CCTV ON COUNCIL LAND

Private CCTV systems are not to be hosted on council land, unless prior written approval is given by the Council's Chief Executive Officer.

GUIDELINES

1. The protection of an individual's privacy shall be maintained by:

- Adhering to Principle 1 of the Act[1] that specifies information can only be collected for a necessary and lawful purpose (i.e. related to the Council's business).
- Adhering to Principle 3 which says that the Council should take reasonable steps to make individuals aware that information is being collected and the reason for that.
- Ensuring that information is collected in a fair manner, in accordance with Principle 4.
- Requiring the appropriate storage and security of recorded information, in accordance with Principle 5.
- Upholding Principle 10, ensuring information is only used for the purpose(s) it was collected.
- Complying with Principles 6, 9 and 11 relating to access to, and retention and disclosure of, information.

2. Information collected from CCTV will only be used:

- To identify and investigate criminal activity or suspicious behaviour with regard to the purposes of this policy.
- For council bylaw enforcement.
- To assist in the operational effectiveness and safety of Council facilities and services.

3. CCTV data will be viewed as close as possible in time to any incident occurring.
4. Only approved persons (as authorised by the Chief Executive and the Council's Privacy Officer, or officers delegated that responsibility by them) or sworn members of the Police with appropriate authorisation will have access to the CCTV data.
5. Access to, or release of, CCTV data requires the agreement of two (2) authorised staff (the Chief Executive and the Council's Privacy Officer, or an officer delegated that responsibility by them).
6. The Council, its staff, contractors and the public are to be informed of the CCTV systems' existence through notices to staff, Public Notices in local media and signage at CCTV locations.
7. This Policy will be used alongside Council employment contracts and codes of conduct.

REQUIREMENTS

NEED FOR CCTV

1. Any new CCTV system or cameras will be installed only where doing so is in accordance with the rationale, purposes and guidelines of this policy.
2. Information will be gathered to help verify whether or not there is a need for any proposed new CCTV installations not covered by the attached schedule
3. Prior to installation of any new CCTV system or cameras, the Council will carry out such consultation as is appropriate (in accordance with Part 6 of the Local Government Act 2002) given the circumstances and nature of the proposed CCTV system or cameras.
4. For existing and new CCTV systems and cameras, the Council will maintain a log detailing access to CCTV, the purpose of access and the operator.
5. The need for CCTV, and its effectiveness, detailing CCTV use and any issues relating to its deployment will be reviewed within 3 years and then reported to the Privacy Commissioner as appropriate or required.. The policy itself will be reviewed every five years, and the review shall include evidence for or against ongoing need, quantified benefits and public consultation.

---

1 See attachment

FAIR USE OF CCTVS

6. Signage advising of CCTV installation will be installed on entries to the areas of camera coverage.

7. CCTV coverage will not include private areas within public spaces and facilities (e.g. locker rooms).

8. CCTV coverage will not be directed at private property, or land designated for Defence or Correctional facilities, without the prior consent of the occupant(s), although some incidental coverage of private property may be unavoidable (e.g., background to a road, private property immediately adjacent to Council property).

9. Covert systems will not be employed unless at the direction of the Police under an appropriate authority or for the Council's internal purposes where there is strong suspicion of criminal activity, or misconduct which may give rise to a health or safety risk to any person or damage to the environment, and which cannot be detected by other means.

PURPOSE OF CCTV/USE OF RECORDED MATERIAL

10. CCTV will only be installed and used for any one or more of the following purposes:

- Property protection;
- Safety and security of public, Council, their staff and contractors;
- Council by-law enforcement, to assist in the operational effectiveness and safety of Council facilities or services; and,
- Law enforcement.

NO DISCLOSURE

11. The Chief Executive and the Council's Privacy Officer, or officers delegated that responsibility by them, may approve persons or entities that data may be disclosed to. A list of all approved persons or entities will be maintained by the Council.

12. Except as provided below under the Local Government Official Information and Meetings Act 1987 (LGOIMA) or as authorised by the Privacy Act, CCTV data will not be disclosed to any person or organisation other than the approved persons listed.

13. Police may be given access to the data as required or requested for law enforcement purposes. The Police's use of any data will be governed by the Privacy Act.

14. CCTV data may include information covered by the Local Government Official Information and Meetings Act 1987 (LGOIMA). In deciding on any official information request under LGOIMA for CCTV data the Council will pay particular regard to the privacy interests of individuals. Such release would not generally be one of the purposes for which the information was collected.

15. Any data released must be authorised by the Chief Executive and the Council's Privacy Officer, or officers delegated that responsibility by them.

STORAGE AND SECURITY

16. The Council will supplement this policy with Operational Guidelines dealing with (amongst other things):

(a) the secure storage of CCTV data;

(b) protocols regarding access to and use of CCTV data within the Council;

(c) the process for and identification of appropriate "approved persons" within the Council (including any contractor providing services relating to CCTV cameras) with specified levels of authority in relation to access to and use of CCTV data; and external persons or entities to whom data can be released;

(d) the period/s that CCTV data will be retained;

(e) disposal and erasure of any CCTV data;

(f) provisions relating to contractors providing services in connection with CCTV cameras.

17. No recorded images or sound will be removed from the system, or copied, unless approved by an approved person (as specified in clause 11). This is to be recorded in the system log, once authorisation has been obtained.

18. Any system misuse will be reported in writing to the relevant approved person and the manager responsible for the business unit, for appropriate action.

19. System checks will be carried out regularly. Any defects will be remedied as soon as practical.

GLOSSARY OF TERMS

Approved persons – Persons approved under the operational guidelines who are allowed access to the systems and data.

Cameras – Any device that has the ability to provide a live view of an area or provide images that can be recorded.

Camera coverage – The areas within the view of the camera.

CCTV – Closed Circuit Television System including all system components making up the system.

Covert CCTV system – A CCTV system that is recorded, without the cameras or recording equipment being apparent to the occupiers and users of the area under surveillance by cameras.

Data – Electronic or other forms of images, footage or sound from the CCTV systems or alternative recording devices.

Data is not compromised – That the recorded data is not altered or manipulated making it unusable or not in its original state.

Log – Record of access the system detailing reason and person.

Recorded data – Camera footage or sound from the CCTV system.

Signage – Signs installed that identify the use of CCTV is use.

Storage and security – That data is stored in an appropriate way reducing the likelihood of accidental loss of or unauthorized access to the data**.**

Viewing equipment – Monitors of similar that display either live cameras or historic recorded data.

ATTACHMENT 1 STATUTORY PROVISIONS

RELEVANT PRIVACY PRINCIPLES

Part 2[2]

Information privacy principles

6 Information privacy principles

The information privacy principles are as follows:

Principle 1 - Purpose of collection of personal information

Personal information shall not be collected by any agency unless—

(a) The information is collected for a lawful purpose connected with a function or activity of the agency; and

(b) The collection of the information is necessary for that purpose.

Principle 3 - Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of—

(a) The fact that the information is being collected; and

(b) The purpose for which the information is being collected; and

(c) The intended recipients of the information; and

(d) The name and address of—

(i) The agency that is collecting the information; and

(ii) The agency that will hold the information; and

(e) If the collection of the information is authorised or required by or under law,—

(i) The particular law by or under which the collection of the information is so authorised or required; and

(ii) Whether or not the supply of the information by that individual is voluntary or mandatory; and

(f) The consequences (if any) for that individual if all or any part of the requested information is not provided; and

(g) The rights of access to, and correction of, personal information provided by these principles.

(2) The steps referred to in subclause (1) of this principle shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(3) An agency is not required to take the steps referred to in subclause (1) of this principle in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

(4) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,—

---

2 The Privacy Act (1993)

(a) That non-compliance is authorised by the individual concerned; or

(b) That non-compliance would not prejudice the interests of the individual concerned; or

(c) That non-compliance is necessary—

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or

(d) That compliance would prejudice the purposes of the collection; or

(e) That compliance is not reasonably practicable in the circumstances of the particular case; or

(f) That the information—

(i) Will not be used in a form in which the individual concerned is identified; or

(ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

Principle 4 - Manner of collection of personal information

Personal information shall not be collected by an agency—

(a) By unlawful means; or

(b) By means that, in the circumstances of the case,—

(i) Are unfair; or

(ii) Intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 5 - Storage and security of personal information

An agency that holds personal information shall ensure—

(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—

(i) Loss; and

(ii) Access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) Other misuse; and

(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6 - Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled—

(a) To obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) To have access to that information.

(2) Where, in accordance with subclause (1)(b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

Principle 9 - Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

Principle 10 - Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,—

(a) That the source of the information is a publicly available publication; or

(b) That the use of the information for that other purpose is authorised by the individual concerned; or

(c) That non-compliance is necessary—

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or

(d) That the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to—

(i) Public health or public safety; or

(ii) The life or health of the individual concerned or another individual; or

(e) That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(f) That the information—

(i) Is used in a form in which the individual concerned is not identified; or

(ii) Is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(g) That the use of the information is in accordance with an authority granted under section 54 of this Act.

Principle 11 - Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,—

(a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) That the source of the information is a publicly available publication; or

(c) That the disclosure is to the individual concerned; or

(d) That the disclosure is authorised by the individual concerned; or

(e) That non-compliance is necessary—

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or

(f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to—

(i) Public health or public safety; or

(ii) The life or health of the individual concerned or another individual; or

(g) That the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) That the information—

(i) Is to be used in a form in which the individual concerned is not identified; or

(ii) Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act.