

Closed Circuit Television (CCTV) Systems Policy

1. Purpose of this policy

- i. This policy sets out how Manatū Taonga Ministry for Culture and Heritage (MCH) will operate its CCTV systems and the rules MCH staff, and its contractors, will abide by when using the system.

2. Application

- i. This policy applies to the installation and use of CCTV owned and operated by MCH and the use of CCTV by contractors of MCH. The policy applies to all MCH employees and contractors of MCH.
- ii. The policy also has implications for the general public who may enter areas where CCTV is in operation.

3. Background

- i. CCTV or “closed circuit television” refers to camera surveillance systems that capture images of individuals or information relating to individuals. The work of MCH is varied, and in some instances, MCH may use CCTV for the purposes of this work. For example, MCH has cameras in its head office premises, at the National War Memorial and in Pukeahu National War Memorial Park. Contractors may use CCTV for the purpose of ensuring the safety and security of a MCH memorial construction site, or as a means of surveillance activity at memorial sites we look after.
- ii. This policy has been developed from the Office of the Privacy Commissioner’s 2009 CCTV guidance *Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organisations*, available at www.privacy.org.nz.

4. Purpose of CCTV systems

- i. MCH is permitted to operate and use CCTV systems for the purpose of safety and security. This policy does not authorise the operation or use of CCTV for any other purpose.
- ii. In this policy, safety and security purposes involve any of the following:
 - a. the protection of individuals;
 - b. the protection of MCH-owned and/or operated property or premises;
 - c. the protection of a premises or site that MCH undertakes works on or in relation to (including, but not limited to, a construction site for a memorial or a site where an MCH-led event or commemoration is occurring); and
 - d. the protection of property managed or maintained by MCH.

5. CCTV cameras

5.1 Location of CCTV cameras

- i. All CCTV cameras must be positioned to observe public spaces (e.g. public parks, footpaths, streets, interior or exterior public areas) and will not be positioned in a manner that unreasonably intrudes on a person's privacy.
- ii. In cases where a CCTV camera records the interior of a building on a semi-public premises the owner of the premises, or a person responsible for the premises' management, will be informed. A semi-public premise refers to spaces (even if privately-owned) that are accessible to the public during opening hours (e.g. shops, cafes).

5.2 Signage of CCTV cameras

- i. Where CCTV is operated at outdoor locations signage must be displayed at the main access points of the perimeter of the CCTV system's range to notify people that cameras are operating. The signs must make clear who owns and/or operates the CCTV system and the contact details of the owner/operator.
- ii. Where appropriate, the signage may also include some or all of the following information:
 - a. The purpose of operating the CCTV (e.g. why are you recording the footage?)
 - b. Whether you intend to pass the CCTV footage on to others, and if so whom;
 - c. Whether the collection of the information is authorised or required under a particular law; and
 - d. The rights of the individual to access and correct the information.
- iii. Where CCTV is operated at outdoor locations MCH must provide a notice on its website to inform the public it is operating CCTV cameras. The notice should contain the information described in clause 5.2(i) and (ii). If the CCTV system is expected to have a major public impact, MCH should also consider notifying the media.

5.3 Operating times

- i. MCH CCTV operation hours will be assessed on a case-by-case basis, ensuring operating hours are limited to times necessary to achieve the purpose of the CCTV recording. Depending on the circumstances, this may include operation on a continuous basis.

6. MCH management of CCTV recordings

6.1 Security of CCTV recordings

- i. Subject to clauses 6.1(ii) and (iii), CCTV images must only be retained for the minimum time period required to achieve the purpose(s) of the CCTV. This means that each time CCTV is installed (or used for the first time) an assessment must be undertaken to determine what retention period is necessary to achieve the purpose(s) of the CCTV consistent with this policy.

- ii. CCTV images will be automatically overwritten after the minimum period of time determined in accordance with clause 6.1(i). If deemed appropriate, CCTV images should be manually overwritten prior to this time if retention is not necessary to achieve the purpose(s) of the CCTV consistent with this policy.
- iii. CCTV images may be retained for a period of time longer than the minimum period determined in accordance with clause 6.1(i) if the CCTV image is required for evidential purposes.
- iv. For the purposes of clause 6.1(ii), MCH must keep a file note on TRIM that records the period of time after which CCTV images will be automatically overwritten and the method of destruction (ie automatic overwrite).
- v. Servers containing recorded footage will be housed in a secure location with access by authorised MCH staff or contractors only on the authority of Ministry employees: Manager Facilities & Emergency Management, Physical Security Officer or Chief Security Officer.
- vi. A log of access to CCTV recordings must be maintained by authorised MCH staff or MCH contractors. If the log is maintained by MCH staff, access should be logged in the MCH Kayako security ticket system.

6.2 Access to CCTV recordings

- i. Only authorised MCH staff or MCH contractors have direct access to MCH CCTV systems and CCTV recordings.
- ii. Other MCH staff or MCH contractors are only permitted to view CCTV recordings if viewing that recording is relevant to their role within (or for) MCH and is in accordance with the purpose(s) for the operation of the CCTV system.
- iii. MCH shall provide access to, or copies of, CCTV recordings to the New Zealand Police, provided the release is justified by reference to Privacy Principle 11.

6.3 Request to access CCTV recordings by other parties

- i. If MCH receive a request from an individual to access CCTV recordings of themselves, MCH must provide that access unless there is a good reason to refuse the request.
- ii. In considering whether there is good reason to refuse a request, MCH must consider the following:
 - a. Whether the information requested is 'readily retrievable'. For example, if the individual asks for recordings of themselves, but cannot provide a specific time or location, then this information might not be considered readily retrievable.
 - b. Whether access would intrude on the privacy of others captured in the recording. If access would unreasonably breach others' privacy then

access should be refused. In these circumstances, MCH should consider whether it could provide the individual with a written description of what they are doing in the footage.

- iii. If MCH accepts an individual's request to access CCTV recordings of themselves, access should be provided in the manner the individual requested, unless it is not possible or desirable to do so. For example:
 - a. if others are pictured in the footage, it may be appropriate to blur/pixelate the faces of others before releasing a copy of the footage; and
 - b. if providing a copy could be damaging or embarrassing for others who are pictured if it is put on the internet, it may be more appropriate to provide access by allowing the individual to come in and view the footage rather than releasing a copy.
- iv. MCH must respond to a request for CCTV recordings as soon as reasonably practicable, but no later than 20 working days.² The response must set out whether or not the request has been accepted, the reasons why, and, in circumstances where the request is accepted, the manner in which access is provided.

7. Privacy

- i. MCH will maintain the protection of individual's privacy by:
 - a. Ensuring CCTV recordings are only collected for the purpose(s) set out in clause 4 of this policy.
 - b. Ensuring CCTV recordings are only used, stored and disclosed for the purpose(s) for which it was collected, unless one of the limited exceptions apply. The limited exceptions include where the use or disclosure is necessary to enable a public sector agency (e.g. the Police) to uphold the law (e.g. investigation of an offence), or where the use or disclosure is necessary to prevent or lessen a serious threat to public health and safety or the life or health of an individual.
 - c. Ensuring CCTV operation hours are limited to times necessary to achieve the purpose of the CCTV recording.
 - d. Taking reasonable steps to make individuals aware of the recording and the reason of the recording.
 - e. Complying with Principles 6 and 9 of the Privacy Act relating to access to and retention of information.

8. Review

- i. The MCH Privacy Officer, MCH Physical Security Officer and MCH Chief Security Officer may review MCH's operation of its CCTV system for the purposes of monitoring compliance with this policy and/or determining whether the CCTV system remains effective.

9. Complaints

- i. Complaints regarding any aspect of the operation of CCTV cameras, including any complaint arising under this policy, shall be directed in the following way:
 - a. Any complaint that relates to privacy should be directed to the MCH Privacy Officer. After receiving a complaint, the MCH Privacy Officer must notify the Manager (Facilities and Emergency Management).
 - b. Any other complaint should be directed to the MCH Privacy Officer and the MCH Physical Security Officer.
- ii. Complaints will be investigated in accordance with the MCH Privacy and Personal Information Policy and related procedures.
- iii. If the complaint relates to an issue of privacy, a complaint may also be made to the Privacy Commissioner.

10. Authority of the policy

The MCH Privacy Officer and the Manager (Facilities and Emergency Management) are the policy owners and are responsible for the implementation and maintenance of the policy.