

CCTV USE AND ACCESS POLICY

1. Application of policy

1.1 This policy applies to the CCTV System to be implemented in the UWA Student Guild Tavern and is a policy of the Guild Council.

2. Definitions

“Authorised User” means a person authorised to view CCTV Footage and approve External Access Requests. In this instance, Authorised Users refer to the Guild Tavern Manager and Guild Managing Director, or another individual nominated by the Licensee. The Authorised Users must have completed CCTV training and be conversant with this policy and applicable legislation.

“CCTV” refers to a Closed Circuit Television System used by the Guild.

“CCTV Footage” refers to any digital image and related data captured by, stored in and recoverable from the CCTV System in the Tavern.

“CCTV System” refers to the CCTV cameras and any other related equipment, including viewing monitors, that will be installed in the Tavern.

“External Access” refers to applications from bodies external to the Guild to view and copy the CCTV Footage.

“Guild” refers to the UWA Guild of Undergraduates, Student Guild or UWA Student Guild as it may be known.

“Incident” refers to an event or circumstance that constitutes, or that the Authorised User believes may constitute or involve any element of, or evidence of the commissioning of a crime, misconduct or disorder.

“Licensee” refers to the body holding the Liquor License. In this case, this refers to the Guild.

“Tavern” refers to the UWA Student Guild Tavern.

3. Purpose

3.1 The purpose of this policy is to govern the use of the CCTV System as an Incident risk management tool, and to limit access to the CCTV System and CCTV Footage to only Authorised Users.

3.2 This policy sets out the procedure for access to CCTV Footage and the reporting of this access.

4. Objectives

4.1 The objectives of this policy are to:

- a) ensure the safety of Guild staff and/or individuals engaged by the Guild in work at the Tavern, security guards and patrons of the Tavern;
- b) ensure the protection of the Tavern premises;
- c) discourage unlawful activity; and
- d) assist in the prevention, detection and punishment of crime.

5. Compliance with Legislation

5.1 This policy is to be read with and is to follow the *Surveillance Devices Act (1999)*.

6. Access to CCTV Footage

6.1 CCTV Footage must only be used for the purposes of investigating and providing evidence of an Incident.

6.2 CCTV Footage will not be viewed unless there is a reported Incident.

6.3 Access to recorded CCTV Footage for the purposes of viewing or disclosing the CCTV Footage to external bodies will be restricted to Authorised Users.

7. External Access Applications

7.1 External Access to CCTV Footage can only be requested:

- a) by the Australian Federal Police;
- b) by the Western Australian Police;
- c) by the Department of Racing, Gaming and Liquor;
- d) under a Federal Court Order; or
- e) under a Western Australian Court Order.

7.2 External Access requests must be directed to Authorised Users. This request must be in writing except in case of emergency where the Authorised User must record the name or badge number, Incident or job number and any other relevant identifying information of the request.

7.3 An emergency could be where a police crime scene has been set up, or is likely to be set up, however the Authorised User has discretion to make the decision as to whether a case is an emergency. Where an emergency is identified, the Authorised User must include this in the report to Guild Council mentioned in 7.6.

7.4 Authorised Users must comply with all requests from these external bodies.

7.5 Individuals may not request CCTV Footage of themselves, except through the above external bodies.

7.6 Authorised Users must report any successful External Access applications to the Guild Council at the next Guild Council Meeting.

8. Footage Requirements

- 8.1 The CCTV System must provide footage that enables identification of all people entering and exiting the premises.
- 8.2 Any CCTV Footage that is collected, viewed or released to third-parties must include the following identifiers:
 - a) Time/date stamp;
 - b) Camera location;
 - c) Camera identifier; and
 - d) Watermarking or method of identifying the original CCTV Footage for authenticity ensuring tamper prevention.

9. Storage and disposal

- 9.1 Any recorded footage of Incidents must be stored in a secure location with access restricted to the Authorised Users.
- 9.2 The Tavern Manager will be responsible for the secure storage of CCTV Footage.
- 9.3 CCTV Footage must be protected from unauthorised viewing, copying, alteration, deletion and disclosure.
- 9.4 CCTV Footage will be stored for a maximum of twenty-eight (28) days, or such period as the Director of Liquor Licensing specifies, before it will be overwritten.
- 9.5 Where CCTV Footage has been provided to a third party, it is that third party's responsibility to retain the record of footage. The Guild will not keep this footage beyond the time frame set out in 9.4 unless required to do so under law, an ongoing formal investigation or Court Order.

10. Public Awareness

- 10.1 CCTV cameras will be clearly visible.
- 10.2 Signs will be at each entrance to notify people that they may be under surveillance.

11. Placement of Cameras

- 11.1 CCTV cameras are to be located at each entry and exit.
- 11.2 The placement of other CCTV cameras will be determined by the Authorised Users, taking into consideration:
 - a) Lighting levels;
 - b) Foot traffic;
 - c) Vision provided by the cameras;
 - d) Accessibility of equipment for repair requirements; and
 - e) Cabling routes and distances.

12. Audio Recording

- 12.1 The CCTV System will not record audio data.

13. Inappropriate Use or Breach of Policy

13.1 Failure to comply with this policy will result in disciplinary action being taken against all involved individuals. The Guild may use any and all evidence to report a failure to comply to the Police or the relevant body.

14. Annual Review

14.1 The Authorised Users will undertake an annual review of the effectiveness of the CCTV System.

14.2 Items considered will include:

- a) The CCTV System's ability to serve its original purpose; and
- b) An assessment of the need for an addition to, the removal of, or the relocation of CCTV cameras.