

## Closed Circuit Television and Surveillance Policy

<b>Approving authority</b>	University Council
<b>Approval date</b>	6 August 2018 (3/2018 meeting)
<b>Advisor</b>	Director, Campus Life <a href="mailto:n.collier-jackson@griffith.edu.au">n.collier-jackson@griffith.edu.au</a>   (07) 373 57592
<b>Next scheduled review</b>	2022
<b>Document URL</b>	<a href="http://policies.griffith.edu.au/pdf/Closed_Circuit_Television_and_Surveillance_Policy.pdf">http://policies.griffith.edu.au/pdf/Closed Circuit Television and Surveillance Policy.pdf</a>
<b>TRIM document</b>	2018/0000063
<b>Description</b>	This policy provides information on the use of surveillance on Griffith University property.

### Related documents

[Griffith University Act 1998 \(Qld\)](#)

[University Campus Use and Access Policy](#)

[Right to Information Act 2009 \(Qld\)](#)

[Information Privacy Act 2009 \(Qld\)](#)

[Invasion of Privacy Act 1971 \(Qld\)](#)

[Workplace Surveillance Act 2005 \(NSW\)](#)

[Information Security Policy](#)

[Griffith University Privacy Plan](#)

[University Sector Retention & Disposal Schedule \(QDAN601\)](#)

[Internal Charges Policy](#)

[Research Centres and Institutes Policy](#)

[Guidelines for the Use and Management of Closed Circuit Television \(CCTV\) systems](#)

[CCTV Installation Request Form](#)

[\[Interpretation\]](#) [\[Introduction\]](#) [\[Purpose\]](#) [\[Control and Deployment of the CCTV System\]](#) [\[Covert Images and Data\]](#) [\[Storage, Use and Disposal of CCTV Footage\]](#) [\[Annual Review\]](#)

## 1. INTERPRETATION

The following definitions are used in this Policy:

- 1.1 **'Authorised Person'** has the same meaning as in Schedule 2 of the Griffith University Act 1998;
- 1.2 **'CCTV'** means closed circuit television systems together with any other form of surveillance technology deployed by the University from time to time.
- 1.3 **'CCTV Footage'** means, at any time, any digital, video and sound images and related data captured by, stored in and recoverable from the CCTV System. CCTV Footage does not include lectures published through the University's system for recording and publishing lectures and teaching materials, or recorded footage used for training purposes.
- 1.4 **'CCTV System'** means the CCTV system (including related components of the University's data network) employed by the University on its Sites or another secure location externally hosted, subscribed, or leased by the University from time to time. The CCTV System does not include infrastructure used to record and publish lectures and teaching materials, including training footage.

- 1.5 'Crime Enforcement Authority'** means the Queensland Police Service (QPS), the Australian Federal Police (AFP), the Crime & Corruption Commission (CCC) and any other public organisations, authorities or agencies entrusted with a law enforcement function.
- 1.6 'Element'** means any school, faculty, or department within an Academic Group and includes all Griffith University Research Centres (as defined in Section 5.0 of the [Research Centres and Institutes Policy](#)) and colleges, and any Administrative Office within an Administrative Division.
- 1.7 'Facilities Optimisation Purpose'** means the use of CCTV to monitor traffic flow also utilisation of teaching and learning spaces so that the University's physical assets may be used in the most efficient and effective manner.
- 1.8 'Guideline'** means the **Griffith University Guideline for the use and management of closed circuit television (CCTV) systems**
- 1.9 'Incident'** means an event that constitutes, or that the Responsible Officer believes may constitute or involve any element of, or evidence of the commissioning of a crime, misconduct or disorder.
- 1.10 'Investigating Officer'** means an Authorised Officer or any other employee, consultant or agent of the University charged with conducting an Investigation.
- 1.11 'Investigation'** means an investigation conducted by or on behalf of the University into a suspected crime, an incident of misconduct or a disorder which has been conducted on a Site or which has impacted on the University's operations.
- 1.12 'Misconduct'** means:
- illegal activity;
  - irregular or unauthorised use, or substantial mismanagement, of University funds or resources;
  - conduct that causes a substantial risk to health or safety, or to the environment; or
  - that a University employee or officer is guilty of maladministration in, or in relation to, the performance of official functions; and
  - includes any breach of the University's statutes, policies or procedures.
- 1.13 'Principal Purposes'** means those purposes described in section 3.1 of this Policy.
- 1.14 'Responsible Officer'** means that person at the relevant time bearing the office of Director, Campus Life, together with any person acting in that role from time to time.
- 1.15 'Site'** includes any land or part thereof which for the time being is the property of the University or in its possession or under its control, together with any structure of any kind whether permanent or temporary on that land;

The definitions used in the Griffith University Act 1998 also apply to this Policy, unless stated otherwise.

---

## 2. INTRODUCTION

The University protects its Sites and the buildings and physical property on those Sites in accordance with the Security Framework. Notwithstanding this, the open and accessible nature of the majority of its buildings and Sites has resulted on occasion in damage and loss of the University's property and assets and/or unauthorised access to Sites. The utilisation of teaching space is a key to both increasing efficiency of existing space and informing the University about future space needs.

To deter and protect its property and assets and measure the utilisation of specific spaces and assets the University employs a CCTV System. This policy sets out the basis upon which that CCTV System is operated, and how CCTV Footage is collected, stored, used and disposed of.

---

## 3. PURPOSE

The University's CCTV System serves the following principal purposes:

- To prevent crime, misconduct and disorder by acting as a psychological deterrent to potential offenders;

- To aid the detection of crime, misconduct and disorder and enable a greater proportion of crime to come to the attention of Crime Enforcement Authorities or security personnel;
- To enhance the apprehension and successful prosecution of offenders by facilitating the gathering of evidence;
- To reduce the likelihood of theft or damage to University property or assets;
- To detect unauthorised access and unethical tissue use as required under the Transplantation and Anatomy Act and Regulations and
- To monitor utilisation of teaching and learning spaces so that the University's assets may be used in the most efficient and effective manner.

This policy does not apply to the recording, audio and screening of lectures which are made available in the relevant Learning@Griffith course site.

---

#### **4. CONTROL AND DEPLOYMENT OF THE CCTV SYSTEM**

The Responsible Officer has overall responsibility for managing compliance with this Policy, including day-to-day management of the CCTV System, training of all Campus Life staff associated with the use of CCTV systems. The CCTV System is under control of the Responsible Officer. The Responsible Officer may delegate any of the responsibilities imposed upon the Responsible Officer by this Policy.

The CCTV System consists of a number of CCTV cameras positioned both internally and externally at various locations on University property. Some CCTV cameras are connected to video image recording equipment which continuously records activities in that area for a specified period of time. Some CCTV systems, particularly those in teaching spaces, are connected to (and CCTV Footage generated by them is stored within) the University's data network or another secure location externally hosted, subscribed, or leased by the University. In exceptional circumstances, CCTV live image viewing can occur in those spaces where live image viewing must be undertaken to meet the principal purpose and is approved by the Vice President (Corporate Services).

All CCTV Footage captured by the components of the CCTV System deployed in teaching spaces are converted to a de-identified image which is used to determine room occupancy in the context of the Facilities Optimisation Purpose.

CCTV installations must not be made without the prior written approval of the Vice President (Corporate Services). Requests for the installation of a CCTV System must be made in writing to the Vice President (Corporate Services) and be accompanied by an explanation of how the installation of the requested CCTV fits with the purposes defined in section 3, and such other information as Vice President (Corporate Services) requests. The Vice President (Corporate Services) may approve or decline to approve any such application on the basis of whether or not the proposed installation would accord with this Policy and represent a benefit to the University commensurate with the installation and ongoing costs involved.

Elements requesting the implementation of CCTV will be responsible for the costs of installation.

CCTV installations made without the prior approval of the Vice President (Corporate Services), or which have not otherwise been authorised by the Vice President (Corporate Services), will be removed at the direction of the Vice President (Corporate Services) at the Element's cost.

The Guidelines on the Use and Management of CCTV systems provides further guidance and defined processes for ensuring compliance with this Policy.

The University's security staff do not monitor the CCTV System on a continuous, regular or sporadic basis although relevant University staff may access the CCTV Footage from time to time in accordance with this Policy when undertaking activities in furtherance of the Principal Purposes.

Except in the unusual circumstance of covert surveillance conducted under section 5 of this policy, CCTV Cameras comprised in the CCTV System will be made visible to staff and visitors. Signs that CCTV cameras are operating are displayed at key positions and in proximity to the area under surveillance to allow people to be made aware that CCTV Systems are operating.

Toilets, showers and change rooms shall not be subject to surveillance by the CCTV System.

Details of overt cameras in the CCTV System and their locations are available from the Responsible Officer upon request. Details of covert cameras are not provided.

CCTV is not deployed on any of the University's facilities situated in the State of New South Wales.

---

## 5. COVERT IMAGES AND DATA

In exceptional circumstances, covert surveillance may be required where there is a concern in relation to the security of an area or there is suspected criminal activity or undertaking.

Covert surveillance will be conducted in a manner which ensured that audio recordings of private conversations are not made in a manner which breaches the Invasion of Privacy Act 1971 (Qld).

Approval in writing must be given by the Vice President (Corporate Services) prior to installation of covert CCTV systems on a Site.

An application to undertake covert CCTV surveillance may only be made by an officer of the University. When seeking written approval to undertake covert CCTV surveillance from the Vice President (Corporate Services), the following information shall be provided in writing to the Vice President (Corporate Services):

- the evidence based grounds for the request (e.g. the identity of the specific person; or
- persons involved in the suspected misconduct, unlawful activities or disorder and the grounds upon which it is believed that person is so involved);
- details of any other managerial or investigative actions which have already been conducted;
- where it is proposed to site the camera;
- who or what will be in view of the camera;
- proposed dates and times of surveillance (which are not to be open ended); and
- an acknowledgement that the University officer making the application has read and understood this Policy;
- an undertaking that there will be no audio recordings made in the course of the covert surveillance; and
- an acknowledgement that the Responsible Officer has been made aware of, and supports the application to undertake covert surveillance.

Any written approval given by the Vice President (Corporate Services) will remain in force for a maximum of 30 days and shall not be used for any other purpose.

---

## 6. STORAGE, USE AND DISPOSAL OF CCTV FOOTAGE

CCTV Footage recorded for a Facilities Optimisation Purpose is converted to a de-identified image and stored on the University's data system or another secure location externally hosted, subscribed, or leased by the University, used to determine room occupancy rates, traffic flows and to otherwise optimise use of the University's physical resources in pursuit of the Facilities Optimisation Purpose. That CCTV Footage will be used and stored in accordance with the University's Privacy Plan and will be disposed of in accordance with University Sector Retention & Disposal Schedule (QDAN601), or any successor retention and disposal schedules.

Otherwise, CCTV Footage will be overwritten (and thus made irretrievable) unless the CCTV Footage is retrieved in response to an Incident. Various components of the CCTV System have differing recording capacities, which vary from 7 to 42 days. Once the recording of the component is exceeded, overwriting will commence so that any given time, the CCTV Footage will extend only to that previous period of time which represents the relevant camera's recording capacity.

Until CCTV Footage is retrieved in response to an Incident or a suspected Incident, the Responsible Officer is responsible for the secure storage of CCTV Footage, which is retained in the CCTV System and securely locked within the physical components of the CCTV System.

Where the CCTV System has recorded information that may relate to an Incident:

- the Responsible Officer may, upon becoming aware of the alleged Incident, direct the CCTV Footage to be retrieved, copied and recorded and provided to an Investigating Officer and/or any Crime Investigating Organisation.
- an Investigating Officer may apply in writing to the Responsible Officer for access to the CCTV Footage in the conduct of an Investigation. Any such application must state the evidence based grounds for the request (e.g. the identity of the specific person or persons suspected to have been involved in the commissioning of a crime, misconduct or disorder and the grounds upon which it is suspected that person or those persons were so involved), the camera location, the date of recording and the time and duration of recording, together with any further information required by the Responsible Officer. Upon being satisfied that there are reasonable grounds for the Investigating Officer to access the relevant CCTV Footage, the Responsible Officer will direct the CCTV Footage to be retrieved, copied and recorded and shown to the Investigating Officer in the company of an Authorised Person, then stored in a locked cabinet and released only for the purposes of the continuing conduct of the Investigation (which may also eventually involve releasing the CCTV Footage to a Crime Investigating Organisation).
- a person who believes themselves affected by an Incident may make written application to the Responsible Officer for that footage to be released to a Crime Investigating Organisation or an Investigating Officer. Any such application must state the evidence based grounds for the request (e.g. the identity of the specific person or persons suspected to have been involved in the commissioning of a crime, misconduct or disorder and the grounds upon which it is suspected that person or those persons were so involved), the camera location, the date of recording and the time and duration of recording, details of the complaint made to the Crime Investigation Organisation or the Investigating Officer, details of relevant contacts at the Crime Investigation Organisation (and written authorisation for the Responsible Officer to contact that person or the Investigating Officer and disclose and seek details of the application and its underlying circumstances), details of any other managerial or investigative actions which have already been conducted and any other information requested by the Responsible Officer. Upon being satisfied that there are reasonable grounds for release of the CCTV Footage, the Responsible Officer will direct the CCTV Footage to be retrieved, copied and recorded and released to the Crime Investigation Organisation or shown to the Investigating Officer in the presence of an Authorised Officer, and then stored in a locked cabinet and released only for the continuing conduct of the Investigation (which may also involve releasing the CCTV Footage to a Crime Investigating Organisation).

CCTV Footage retrieved in response to an Incident will be recorded on a register to be kept by the Responsible Person and will be held in accordance with the University's Privacy Plan and disposed of in accordance with University Sector Retention & Disposal Schedule (QDAN601), or any successor retention and disposal schedules.

In any of the circumstances specified in section 6.4, the Responsible Officer may release the relevant CCTV Footage to the University's legal advisors and Internal Audit Unit.

CCTV Footage will generally not be made available to members of the public, although an individual may request access to CCTV Footage in accordance with the University's Privacy Plan.

---

## 7. ANNUAL REVIEW

The Responsible Officer will cause an annual review to be undertaken of the effectiveness and value for money of each component of the CCTV System used to deter unlawful behaviour, misconduct or disorder. This annual review will be undertaken to assess the need for additional, removal or relocation of CCTV System components and will address, in respect of each component:

- Its ability to serve the purpose for which it was originally installed;
- Incidents of crime/damage detected.

In the context of incidents of crime/damage or loss within the vicinity of the camera and the campus in general.