Edith Cowan University

Close Circuit Television (CCTV)

CODE OF PRACTICE

TABLE OF CONTENTS **Page No.**

Notes:

1. INTRODUCTION

1.1. This document details the Code of Practice that will be applied to the management of the close circuit television system (CCTV) established ECU University by Facilities and Services. The system has been implemented by the University to assist in the protection of staff, students and visitors to the campus as well as providing enhanced security of University assets.

1.2. The CCTV system will be managed in accordance with all relevant external regulations and University policies. The conditions applied to the use of the system, including the storage, disposal and access to images and the storage of information, are detailed within this Code of Practice.

1.3. The Director, Facilities and Services has executive responsibility for the system, including approving any extension of the system within the University. The Director is also responsible for managing adherence with the conditions laid down in the Code of Practice and is the only officer authorised to approve amendments to the conditions of the Code. Any changes or extensions to the Code or System will only take place after consultation with relevant University management. Where specific arrangements are established with an area, a written record of the agreed procedures will be made.

1.4. The Director may authorise an agent to approve minor changes to the system and to this Code, where appropriate. Minor changes are those that do not have a significant impact on the intent of the Code or the procedures established to monitor adherence with its provisions.

1.5. Where appropriate, the Western Australian WAPOL Force will be asked to investigate any matter recorded by the CCTV system which is deemed to be of a criminal nature.

2. STATEMENT OF PURPOSE

2.1. As indicated in the previous section, the CCTV system is intended to provide an increased level of security in the University environment for the benefit of those who study, work, live in, or visit the campus. Subject to this Code of Practice the System will not be used to invade the privacy of any individual. For the purpose of this Code, the University environment includes all University land and buildings, including those areas occupied by Colleges and commercial businesses.

2.2. The CCTV is utilised on an evidentiary basis (archival) and is not monitored for any pre-described duration. All footage is stored on the relevant recording device and accessed on an as needs basis following a recorded incident.

2.3. The system will only be used for the following purposes and within this Code of Practice at all times:

a) To reduce the fear of crime and to reassure the public;

b) To deter and detect crime, criminal damage and public disorder;

c) To identify, apprehend and prosecute offenders in relation to crime, criminal damage, public disorder, road traffic accidents involving serious injury and all forms of harassment;

d) To provide the University, the WAPOL and the Government with evidence upon which to take criminal and civil actions in the Courts;

e) To monitor and assist traffic management issues; and

f) To assist other Emergency Services.

2.4. There may be circumstances where the Western Australian Police Force (WAPOL) wish to conduct a pre-planned operation on the University site. The Director or agent may authorise the use of this system to support these operations, provided it is done within the provisions of this Code and a representative of the WAPOL is present in the Control Room for the full duration of the operation.

2.5. Any use of this system or materials produced which is frivolous, or for private purposes, or is otherwise inconsistent with the objectives and procedures outlined within this Code will be considered gross misconduct. Any University staff member involved in incidents of this type will face appropriate disciplinary action in accordance with the relevant University policies.

2.6. As community confidence in the system is essential, all cameras will be operational. An appropriate maintenance program will be established and under no circumstances will "dummy" cameras be used.

3. SYSTEM USE

3.1. The system will be used to respond to the following key objectives, which will be subject to annual assessment and reports:

a) To detect, prevent or reduce the incidence of property crime and offences against the person;

b) To reduce the theft of cars and theft from cars both on streets and in car parks;

c) To improve general security monitoring in the path areas of the campus, both in terms of personal security and security of premises;

d) To reduce graffiti (particularly offensive graffiti), vandalism and other criminal damage to improve the environment and reduce costs;

e) To prevent and respond effectively to all forms of harassment and public disorder;

f) To assist in traffic management where necessary;

g) Provide emergency service assistance.

4. SYSTEM DETAILS

4.1. The CCTV System consists of a number of overt colour CCTV cameras situated on University property, which continuously record activities in that area. The current locations of cameras on campus are detailed in Appendix 1 (available in hard copy only).

4.2. The Control Room is situated on campus (JO B1.208k) and is capable of receiving images from throughout the area. The Control Room is staffed during core hours by authorised Security Operations staff. The Control Room is also equipped with a licensed radio system linking security officers and the Control Room.

5. DATA PROTECTION – PRIVACY

5.1. All data collected using this system, including images, will be managed in accordance with the provisions of the Commonwealth Privacy Act 1988 and the relevant University policy relating to the control of private information (The University's privacy statement is located at the following URL: (http://www.ecu.edu.**au**/supplemental/privacy).

5.2. All persons involved in the operation of the system must take all reasonable precautions to prevent improper disclosure of material.

5.3. Unauthorised disclosure of CCTV footage is a breach in the University Privacy Policy and may result in disciplinary action under the University Code of Conduct.

6. MANAGEMENT OF THE SYSTEM

6.1. Facilities and Services (ECU Security & Traffic Services business unit) is responsible for ownership of this Code of Practice and Work Instruction.

6.2. Security and Traffic Services is responsible for managing compliance with this Code, including compliance by staff and contractors employed to work on the system or in the Control Room.

6.3. The Manager, Security and Traffic Services, shall be responsible for the day-to-day management of the system and associated processes. In particular, the Manager will be responsible for WAPOL liaison, compliance with the Code of Practice and Work Instruction by staff, contractors or any other authorised person, staff training, the preparation reports and the evaluation of the system performance.

6.4. The Manager will be responsible for managing the Control Room, ensuring that only authorised personnel are given access. A record will be kept of all personnel requesting access to CCTV footage and the Manager will review this record on an as needs basis.

7. EXTENSION OF THE SYSTEM

7.1. Where an agreement is reached to extend the System, the parties (that is the Division and any area affected by the extension of the System) agree to take the following actions:

a) At the outset, they will identify and agree on primary aims and associated issues that must be addressed to achieve those aims.

b) They will identify and plan for resource implications, including deciding the commitment levels of resourcing that will be provided by each participant (client).

c) They will agree to the extent of involvement and respective responsibilities of each party.

d) They will identify any issues that can only be resolved by agreement of all parties participating at that stage of the System (including a decision to change operating priorities to extend the technical capacity of the system).

e) They will establish protocols to govern the process for decision making both in establishing the system within the area and for the ongoing management of the system.

f) They will establish operational procedures for the management of the system and, as appropriate, implement protocols for monitoring and auditing of the System, as it affects those areas.

g) They will draft and sign an agreement outlining the responsibilities of the parties, and in particular, acknowledging the requirement for all parties to comply with the provisions of this Code, including the enforcement of sanctions detailed within the Code.

7.2. Prior to any extension of the System being approved the following actions will be completed:

a) Facilities and Services (Security & Traffic Services) will conduct a needs assessment and prioritisation of risk management objectives.

b) Consultation shall be undertaken between the Security & Traffic Services (STS) and the local areas (and any other parties affected by the extension).

c) Where cameras are to be installed externally STS will consult on an as needs basis with any affected departments.

8. ACCOUNTABILITY

8.1. The University acknowledges the importance of accountability in the management of the system. With that in mind, the following steps will be taken to ensure the campus community is informed:

a) Copies of the Code of Practice will be available to the public via the University web page.

8.2. Any agreement approving WAPOL participation in this System will be subject to both parties complying with the Surveillance Devices Act 1998.

9. PUBLIC INFORMATION

9.1. Cameras will not be hidden and as far as possible will be placed in public view.

9.2. Signs that CCTV cameras are operating may be displayed at key positions. The signs will allow people entering the University to be made aware that CCTV systems operate within the University

10. COOPERATION WITHIN A UNIVERSITY ENVIRONMENT

10.1. The System will operate in a manner that is sensitive to the privacy of people living and working in the area.

11. ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE

11.1. Facilities and Services is responsible for ensuring that the System is evaluated annually by the Director or agent.

11.2. Evaluation will be conducted according to the following criteria:

a) Impact on crime/damage/public order.

b) Impact on key objectives.

c) Impact on neighbouring areas without CCTV.

d) Operation of the Code.

11.3. Ongoing monitoring of the System will be conducted by the Manager, Security and Traffic Services, who will also take all reasonable measures to ensure that all relevant parties are complying with the provisions of this Code.

12. OPERATING STAFF

12.1. This section applies to both University staff and contractors employed to work on the system. Staff and contractors will comply with the following conditions:

a) The employment of staff will comply with all relevant University policies. Contractors will ensure that staff are employed in accordance with relevant industrial awards and legislation, including equal opportunity and occupational health and safety. Contractors will ensure that the selection process provides for thorough validation of the suitability of candidates to work in this environment.

b) Contract staff must be qualified at a suitable level to complete the required duties of the contract work.

c) University staff will be subject to the University disciplinary procedure in the event of actions that do not comply with the conditions of this Code. Where it is proved that contract staff have breached any of the conditions of this Code, these staff will not be permitted to continue working on campus. In appropriate circumstances, the University reserves the right to terminate a contract where a breach of this Code is proved. These conditions will be detailed in all contracts let for services in this area.

d) The Manager Security and Traffic Services will ensure that all University staff will be briefed on their responsibilities under this Code. The Contractor will ensure all contract

staff are briefed regarding the requirements of this Code. Where appropriate, the Facilities and Services Division will a briefing on the conditions of this Code in the Contractor Induction Program run by the Division.

e) A requirement of confidentiality, which can be enforced during and after termination of employment.

f) University management and Contractor managers will establish systems of monitoring and supervision that will ensure compliance with the Code of Practice and operational guidelines.

12.2. All University staff and contract staff must be briefed on the conditions of the Code of Practice and Operational MECUal before commencing work on the system or within the Control Room area.

13. COMPLAINTS

13.1. Complaints regarding the CCTV system and its operation must be made in writing to the Director, Facilities and Services. Where appropriate, the Director will appoint an independent officer with suitable qualifications to investigate the complaint and provide a written report within an agreed period of time. The report will be presented to the Director, Facilities and Services, who will normally take action as appropriate within the University guidelines and then advise the complainant. Where the complainant is not satisfied with the resolution, the complaint can be directed to the Vice-Chancellor for investigation and action as appropriate. For this Code, the definition of an independent officer is one who does not directly work in areas responsible for the management or maintenance of the CCTV system. The investigating officer can be on the staff within Facilities and Services.

14. BREACHES OF THE CODE INCLUDING THOSE OF SECURITY

14.1. Breaches of the Code of Practice and of security must be subject to proper investigation by, in the first instance, the person appointed by the Director to conduct an investigation. This person shall be responsible for making recommendations to the Director to remedy any breach which is proved or evidenced.

14.2. The University reserves the right to apply disciplinary sanctions for breaches, up to and including referring the breach to the WAPOL.

15. CONTROL AND OPERATION OF THE CAMERAS

15.1. Control Room equipment and the remote control of cameras will only be operated by the Manager, Security and Traffic Services, Control Room Staff and persons/staff under training. All these people will act with the utmost probity.

15.2. All use of cameras and recording equipment will accord with the purposes and key objectives of the System, as developed in training and specific operational instructions to staff, and shall comply with this Code of Practice.

15.3. Cameras will not be used to look into private property. Operational procedures shall be adopted to ensure restraints upon the use of cameras in connection with private premises.

15.4. System Operators will be subject to supervisory procedures to ensure compliance with this aspect of the Code.

15.5. System Operators are aware that recordings are subject to routine audit and that they may be required to justify their interest in a member of the public or premises.

15.6. The Manager, Security and Traffic Services will decide the level of incidents to be reported to the WAPOL. The WAPOL shall log all such incidents. It is recognised that the decision as to what level of response is deployed is a matter entirely for the WAPOL. The Manager, Security and Traffic Services will liaise regularly with the WAPOL on this subject.

15.7. The CCTV Work Instruction will provide guidance on the method of operation of cameras, length of time viewing monitors and of minimum operator's performance levels.

16. ACCESS TO AND SECURITY OF THE MONITORS/CONTROL ROOM

16.1. Access to view monitors, whether to operate the equipment or view the images is strictly limited to staff with that responsibility.

16.2. The Control Room will remain locked at all times with an access control point that is secured 24 hours a day via the necessary schedule. Routine access will only be granted to certain Managers, staff, WAPOL Officers and those under training.

16.3. It is important that visits do not interrupt the efficiency of the system. Casual visits will not be permitted. Organised parties shall be allowed for lawful and proper reasons to visit by the Manager, Security and Traffic Services with approval, in advance. The Manager, Security and Traffic Services (or the approved agent) will be present during all organised visits.

16.4. Public access to or the demonstration of monitors will not be permitted except for lawful and proper reasons.

16.5. Visits by no more than two WAPOL Officers at any one time will be permitted provided that they are on duty and the visit is in connection with liaison, training or purposes of the system. These visits must be authorised by the Manager Security and Traffic Services or agent in writing in advance.

16.6. Security procedures will be the subject of audits.

17. DIGITAL / NETWORK VIDEO RECORDERS AND RECORDED MATERIAL

17.1. Recorded material will be used only for purposes defined in this Code of Practice. Access to recorded material will only take place as defined in the Code of Practice. In particular recorded material will not be sold or used for commercial purposes. The showing of recorded material to the public will only be allowed in accordance with the law, either in

compliance with the needs of the WAPOL in connection with the investigation of crime, which will be conducted in accordance with the provisions of any relevant WAPOL and criminal procedures, and any advice and guidance given to the WAPOL from time to time; or in any other circumstances provided by law. Any showing of the material will protect the rights of innocent parties.

17.2. Ownership and copy right of all recorded material vests in the University.

17.3. Recording equipment will be checked from on an agreed schedule by the Manager, Security and Traffic Services to ensure it is in good working order. All recorded images will show the time, date, and camera numbers.

17.4. Digital / Network Video Recorders (DVR / NVR) are to be located in a secure cabinet and access is restricted.

17.5. WAPOL may be given access to CCTV footage where an officer reasonably believes that access and/or copies of specific tapes are necessary for the investigation and detection of an offence or offences, or for the prevention of crime. This is in accordance with the Surveillance and Devices Act 1998. CCTV footage provided to the WAPOL shall at no time be used for anything other than the purpose specified and identified when operators release the evidence to the WAPOL. All requests for access to CCTV footage by WAPOL must be approved by the Manager Security and Traffic Services or the approved agent and an official WAPOL "Receipt of Evidence" must be provided.

18. DEALING WITH INCIDENTS

18.1. The level of WAPOL response to incidents occurring on campus will be determined by the WAPOL and will be subject to the various priorities at the time the incident is reported. The University has no control over the priority allocated by the WAPOL.

18.2. The Control Room operators are authorised to report relevant matters to the WAPOL and other emergency services, as appropriate. A written record of any reports will be made at the time and will include details of the incident, date and time of the report and details of the WAPOL or other services officer taking the report. Where appropriate, the Control Room operator may elect to have the ECU Mobile Security Patrol attend the incident before making a formal report to the WAPOL or emergency services.

18.3. All incidents requiring attendance by the WAPOL or other emergency services will be reported to the Manager, Security and Campus Services, as soon as possible.

19. WAPOL CONTACTS

19.1. The presence of a WAPOL Officer in the Control Room for a pre-planned operation or ongoing incident is permitted, subject to authorization being given by the Director or agent. This Officer may direct the operation of cameras. However, these directions must comply with conditions outlined in this Code of Practice. The Control Room operator has discretion to refuse directions where he/she believes that the request does not comply with the Code.

19.2. There will be no remote control facility at the WAPOL Communications Centre but a WAPOL Officer may direct camera operators during a live incident audibly, by the telephone, provided the actions requested comply with this Code of Practice.

19.3. Should a request from the WAPOL arise for use of the system in any manner that is not provided for by the Code of Practice, this request must be agreed between the Director and the Area WAPOL Inspector concerned. This approval process cannot be devolved to an agent.

19.4. A written record will be maintained of any use of the system at the request of the WAPOL. This record will include details of the WAPOL Officer making the request, details of the Divisional officer authorising the request, time and date of the request and reasons for the request.

20. COMPLIANCE AUDIT

20.1 Compliance by University staff (specifically Control Room staff) and contract staff will be subject to audit. These audits will be conducted as required and at least once per year. The Director, Facilities and Services will appoint an independent staff member to undertake the audit and provide a written report.

21. References

Owner:	Manager Campus Services
Approved By:	Director Facilities and Services Manager, Governance Services
Date Approved:	October 2010
Due for Review:	October 2012
Amendment Dates:	
Related Policies/Documents	Privacy Policy: http://www.ecu.edu.au/GPPS/policies_db/policies_view.php?rec_id=0000000335 Code of Conduct: http://www.ecu.edu.au/GPPS/policies_db/policies_view.php?rec_id=0000000217 Surveillance and Devices Act 1996: http://www.austlii.edu.au/au/legis/wa/consol_act/sda1998210/

22. Contact Information:

Contact Person:	Manager Security Services
Telephone:	6304 2271
Email address:	g.sutton@ecu.edu.au

NOTES:

For Manager, Security and Traffic Services read also Security Systems Administrator or any other Officer so appointed by The Director, Facilities and Services.

Definitions:

***Agent**:* An officer authorised by the Director, Facilities and Services to act on his behalf under this Code of Practice. Normally, Manager Security and Traffic Services unless otherwise stated. *Contractor:* Contractor employed by the University to work on the CCTV system or in the ECU Control Room.

***IRIS**:* The electronic log used by ECU Security to record incidents occurring during a security shift *Operations MECUal:* Any authorised mECUal detailing standard operating procedures for activities undertaken or systems managed by ECU Security.

***WAPOL**:* Western Australian WAPOL Force.

***WAPOL officer**:* Western Australian WAPOL Force Officer.

***Register**:* Transmittal register used to record the transmission, archiving or disposal of tape media containing visual images recorded using the University CCTV system.

***Security Officer**:* ECU Security Officer.

***Staff member**:* University staff member.