Cardiff University
Security & Portering Services (SECTY)
CCTV Code of Practice

Document history

Author(s)			Date	
S Gamlin			23/05/2018	
Revision / Number	**Date**	**Amendment**	**Name**	**Approved by**
BI annual revision				
Date		**Name**	**Approved by**	

1. Introduction. 2
2. Definitions. 2
3. Scope. 2
4. Ownership and Operation. 3
7. Purpose of the CCTV System. 3
8. System Details. 4
9. Installation and Signage. 4
10. Access to Live Footage and Recordings. 4
11 Retention of Recorded Materials and Disposal. 5
12 Breaches of the Code and Complaints. 6
Appendix 1 7
Appendix 2... **7**

1. Introduction.

This Code of Practice aims to ensure that the fixed CCTV systems installed and operated by Cardiff University comply with the law and that the scope, purpose and use of the systems are clearly defined and proportionate.

If at any time mobile cameras are employed, their use will also be governed by this Code of Practice.

2. Definitions.

For the purpose of the Code of Practice the following definitions will apply:

- "University" refers to Cardiff University.
- "CCTV" is Closed Circuit Television System.
- "Security Services" refers to Cardiff University Security Services as part of Security & Portering Services (SECTY).
- "Data Controller" is Cardiff University.
- "Systems Operator" is Head of Security & Portering Services (SECTY).
- "Systems Users" are Security and Library staff authorised to use the Closed Circuit Television System.

3. Scope.

This Code of Practice is binding on all employees and students of Cardiff University and all employees of contracted out services. It also applies to all other persons who may be present, for whatever reason, on Cardiff University property.

4. Ownership and Operation.

The University CCTV system is operated by Security Services, as part of Security & Portering Services (SECTY) whose personnel are employed directly by Cardiff University. There is also a secondary internal CCTV used Datacentre & IT LAN / Computer rooms operated by ARCCA & UITGB staff (appendix 2). These CCTV systems, including all recorded material and copyright are owned by Cardiff University.

The designated Systems Operator of both systems, on behalf of Cardiff University, is the Head of Security & Portering Services.

5. Compliance with Data Protection Legislation

In the administration of its CCTV system Cardiff University will comply with Data Protection legislation in particular the data protection principles set out within Article 5 of the General Data Protection Regulation (GDPR) and as outlined in Appendix 1 of this Code.

6. Application of Data Protection Legislation

- Where images of living, identifiable individuals are deliberately recorded, this is likely to comprise those individuals' personal data. The collection, use and storage of personal data are governed by data protection law. Cardiff University is registered with the Information Commissioner as a Data Controller operating CCTV.

- Data subjects' rights, including a right of access to personal data, (in accordance with article 15 of GDPR), will be respected where recordings are confirmed to comprise personal data. Where an individual requests access to recordings believed to be their personal data, the matter shall be referred to the Assurance Services team in the Department of Strategic Planning and Governance (DOSPG).

- The CCTV system will be operated with due regard for privacy of the individual and in accordance with Article 8 of the European Convention on Human Rights (ECHR) i.e. an individual's right to privacy.

- The CCTV system is fundamentally an overt system, used within the confines of the recognised Cardiff University campus. The CCTV system's existence and presence will be declared as in section 9 of this document.

- Any changes to the purposes for which the CCTV system is operated will require the prior approval of the Deputy Director of Estates Operations in consultation with the Chief Operating Officer and will be published internally as part of this Code at Section 7.

- The use of the CCTV system for any covert purpose must be for exceptional, justifiable and proportionate purposes only, as qualified above, and agreed by the Deputy Director of Estates Operations in consultation with the Chief Operating Officer or designated deputy. In these circumstances details of the change will not be published in advance or disclosed thereafter.

7. Purpose of the CCTV System.

The 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.

The CCTV system will be used to respond to the following legitimate aims / key objectives, which will be subject to bi-annual review or sooner if required.

- To detect, prevent or reduce the incidence of crime.
- To prevent and respond effectively to all forms of harassment and public disorder.
- To improve communications and the operational response of security patrols in and around the areas where CCTV operates.
- To reduce the fear of crime.
- To create a safer community.
- To gather evidence by a fair and accountable method.
- To provide emergency services assistance.
- To assist with health and safety.
- To monitor traffic flow and the use of Cardiff University car parks.
- See Appendix 2 for Datacentres and IT LAN / Computer rooms.

As community confidence in the system is essential, all cameras will be operational. An appropriate maintenance programme will be established.

8. System Details.

The CCTV system consists of in excess of 500 overt colour cameras situated on University property, which continuously record activities in that area, their location contained within our asset location list. Any camera that is deemed to be not required will be switched off or removed.

Monitoring will take place in the Security Control Room which is staffed 24 hours a day by Security members of Security & Portering Services (SECTY) working in shifts.

9. Installation and Signage.

Cameras shall be installed in such a manner as not to overlook private domestic areas. Cameras shall not be hidden from view and signs will be prominently displayed in the immediate locality of the cameras where possible and on entry to zones where CCTV is in operation i.e. entrance to a building.

The signs will indicate:

- The presence of monitoring and recording.
- The ownership of the system.
- Contact telephone number.

10. Access to Live Footage and Recordings.

10.1 Access to Live Footage.

Images captured by the system will be monitored in the Security Control Room, a self-contained and secure room on the Cathays Campus. For operational purposes, and in accordance with the stated purposes of the system, only designated Security staff from Security & Portering Services (SECTY), trained in their duties, shall have access to live CCTV footage. These staff will be referred to as Systems Users.

See Appendix 2 for Datacentres and IT LAN / Computer rooms.

Non-essential access to the Security Control Room is monitored / controlled and all staff are trained in their responsibilities in respect of the use of CCTV.

10.2 Access to Recordings.
For operational purposes and in accordance with the stated purposes of the system, only designated Security staff from Security & Portering Services (SECTY) shall have primary access to all CCTV recordings.

(See Appendix 2 for Datacentres and IT LAN / Computer rooms.)

The Head of Security & Portering Services (SECTY) or nominee may permit the viewing of the CCTV recorded materials by other University staff where this is necessary in connection with the prevention of crime, assisting in the apprehension and prosecution of offenders or matters of national security.
Where University staff request access to CCTV recorded materials for any other purpose, the matter shall be referred to the Assurance Services team in the Department of Strategic Planning and Governance (DOSPG).

10.3 Disclosure of Recorded Material.
As the main purpose of the CCTV system is to prevent crime and assist in the apprehension and prosecution of offenders, designated Security staff from Security & Portering Services (SECTY) may release CCTV recorded materials to the police where Cardiff University has initiated contact with the police and there is a reasonable belief that the CCTV recorded materials will be of assistance.

Where the police or other official investigative body with prosecuting powers approach Cardiff University and request access to CCTV recorded materials they shall be asked to provide a formal notice in writing confirming that the information is necessary for either the prevention/detection of crime or the apprehension or prosecution of offenders, or matters of national security.

Where any other person requests access to CCTV recorded materials, this request shall be forwarded to the Assurance Services team in the Department of Strategic Planning and Governance (DOSPG).

In all cases where recorded materials are disclosed outside the University, the appropriate Security & Portering Services (SECTY) officer shall ensure that the disclosure is logged and duly signed for.

(See Appendix 2 for Datacentres and IT LAN /Computer rooms.)

11. Retention of Recorded Materials and Disposal.
CCTV recordings and other materials produced from them shall be retained for fourteen days (in the case of DVD Hard Disc recordings) unless an incident is recorded which requires further investigation either by the Security Service as part of Security & Portering Services, the police or another external body with prosecuting powers.

In the latter case, recordings shall be kept for a period of three years from the date of recording.

All media, on which recordings were made, that are no longer required will be securely destroyed and the appropriate details entered in the Destruction Records.

See Appendix 2 for Datacentres and IT LAN / Computer rooms.

12. Breaches of the Code and Complaints.

A copy of this Code of Practice will be made available to anyone requesting it and on the University website. Any complaint concerning misuse of the system will be treated seriously and investigated by the Head of Security & Portering Services or nominee with advice from the Assurance Services team in the Department of Strategic Planning and Governance (DOSPG) as appropriate.

The Head of Security & Portering Services or nominee will ensure that every complaint is dealt with under the Cardiff University Customer Complaints Procedure which includes a written acknowledgement of the complaint within three working days. Further details about the process of dealing with complaints can be found in the Customer Care Policy and Procedure.

Breaches of this Code of Practice shall be dealt with in accordance with the appropriate disciplinary policy. Serious breaches of the Code may result in criminal liability on behalf of the individual which could be considered as gross misconduct.

Where appropriate, consideration will be given as to whether the police will be asked to investigate any matter relating to the CCTV system which may be deemed to be of a criminal nature.

Reviewed and amended in accordance with Home Office guidance ‘Surveillance Camera Code of Practice ~ Section 30(1) (a) of the Protection of Freedoms Act 2012.

Appendix 1

Data Protection Principles.

Processing shall be taken to mean all operations including obtaining, recording, storing, analysing or converting into other formats.

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and where necessary kept up to date;
- Kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Appendix 2

Datacentres and IT LAN / Computer rooms CCTV System (ARCCA & UITGB)

1. Introduction.

    - In support of security across the campus various data centres and computer rooms have secondary CCTV systems tailored to the needs of the UITGB and ARCCA that operate entirely within the data centres and computer rooms with no external functionality. It is an overt system and is displayed as such.
    - The Codes of Practice that precede this appendix also apply to the use of the Datacentre & IT LAN / Computer room system. The following additions are specific to that use.

2. Definitions.

    - ‘System User’ includes UITGB and ARCCA staff briefed and authorised to use the Datacentre and computer room systems only.
    - The dedicated ‘Systems Operator’ for the UITGB and ARCCA systems is the Head of Security and Portering Services.

3. Purpose.

    - Specifically in relation to UITGB and ARCCA the purpose of its CCTV system is for the monitoring of the environment and behaviour in accordance with datacentres and computer room rules, security, health & safety of UITGB and ARCCA staff, and monitoring of damage and theft of property.

4. Installation and signage.

    - UITGB and ARCCA will adhere to the preceding guidance about signage as the data centres and computer rooms have external contractors working in these areas.

5. Access to live footage.

    - Access to live footage on the Datacentre and IT LAN room system is restricted to authorised System Users only i.e. UITGB and ARCCA staff authorised to use the system, plus designated Security staff from Security and Portering.
    - These images will be monitored on an on-going basis on display screens in the UITGB Operations room and Data Centre Support Offices and shall not, as far as is reasonably possible, be visible to non-authorised personnel (note: these are not public access areas).

6. Access to Recordings.

    - Access to recordings shall only be given to designated UITGB, ARCCA and Security staff.
    - Preceding guidance on the access of other staff to recordings will be strictly adhered to. (Permission of Head of Security).

7. Disclosure of Recorded Material.

    - UITGB and ARCCA staff shall not disclose CCTV recorded material to any other person or authority without the permission of the Head of Security. Such requests will be dealt with under the preceding process via Security and Portering.

8. Retention of Recorded Materials and Disposal.

    - UITGB and ARCCA CCTV recordings and other materials produced from them shall be retained for 3 months unless an incident is recorded that requires further investigation by an appropriate body. In the latter case, recordings shall be kept until no longer required.

    - UITGB and ARCCA staff will delete the files from the server storing the CCTV recording and appropriate details regarding the operative and date will be recorded in the Operations monitoring logs (acting as a record of destruction).This will be reviewed by the Head of Security or their designated representative who will authorise the monitoring log record.

    - The records of destruction and any retained footage will be reviewed to ensure compliance with the principles of the national code of practice for the management of CCTV every 6 months by the Head of Security or their designated representative.

9. Breaches of the Code and Complaints.

    - The complaints process that precedes these appendices will be applicable to the UITGB and ARCCA systems and their authorised users.