CLOSED-CIRCUIT TELEVISION (CCTV) POLICY

1 Introduction

The purpose of this Policy is to ensure that the University of Aberdeen, as the Data Controller in terms of the Data Protection Act 1998, operates its CCTV or similar systems in a way that complies with the law and that the scope and responsibilities for the systems are clearly defined.

2 Overview

The use of CCTV is intended to provide an increased level of security in the University environment for the benefit of those who visit, study, work or live on the campus.

3 Scope

This Policy governs the installation and operation of fixed Closed Circuit Television (CCTV) cameras and systems operated by the University of Aberdeen on its campuses. If at any time mobile cameras are employed, their use will also be governed by this Policy.

This Policy applies to all University of Aberdeen employees, students and all employees of any contracted out services. It also applies to all other persons on University of Aberdeen property.

The Policy is based on the Code of Practice for surveillance cameras and personal information[1], issued by the Information Commissioner's Office (ICO), under the Data Protection Act 1998. It also reflects established best practice in the management of CCTV systems.

4 The Policy

The key principle for the Policy is to ensure that any CCTV system used on University campuses is operated with due regard for the privacy of the individual and the University's legal obligations, particularly under the Data Protection Act 1998 and appendices 2 and 3 of the ICO Code of Practice referred to above. This policy should be read in conjunction with the University's Policy on Data Protection.

5 Purpose of the CCTV System

The University uses CCTV for the following purposes:

- Assist in the prevention and detection of crime;
- Facilitate the identification and prosecution of offenders;
- To gather evidence by a fair and accountable method;
- Assist in providing a safe and secure environment for the benefit of those who visit, study, work or live on the campus;
- Protect University Security staff from threats and violence;
- Assist in safeguarding University Security staff (and any other persons in the vicinity) during deployments to incidents or emergency situations;
- Monitor crowd movements during University events;
- To assist with Health and Safety;
- Provide the Police, Health and Safety Executive, and University with evidence upon which to take criminal, civil or disciplinary action respectively.

[1] https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

The use of CCTV for any purpose other than those outlined above must be approved by the Data Controller's Representative (Secretary to the University) together with the Director of Estates or their nominees in consultation with the University Data Protection Officer.

6 System Details

- Cameras are located throughout the University's campuses and within its buildings. These locations may change or be added to dependent upon the requirements of the University.
- The system operates 24 hours a day, 365 days per year.
- To ensure privacy, wherever practicable cameras are prevented from focusing on private property.
- The University's Security Control Room will be the only location where the images can be recorded and if any images are to be recorded the recording will take place within the Security Control Room.
- Images will be held in a data base for no longer than is necessary. This period is currently 21 days after which the images will be automatically and securely erased unless there is a recorded and proportionate reason for their longer retention.
- Signage will be appropriately displayed in the locality of the cameras indicating the presence of monitoring and recording equipment and detailing ownership of the system.

7 Covert Surveillance

Any covert surveillance must be authorised in advance by the University Secretary and the Director of Estates or their nominees in writing. This will be undertaken in consultation with the Director of Human Resources, the Security Manager, or Data Protection Officer, as appropriate.

Covert surveillance may only be used if the following criteria are met:

- Its use is part of a specific investigation;
- There are grounds for suspecting criminal activity or equivalent malpractice;
- The use of CCTV is the only reasonable way to investigate the matter;
- Informing people about the monitoring would impede the effectiveness of the monitoring;
- The cameras are not in "private areas" such as toilets or individual offices (except in the case of suspected serious crime with the intention of assisting the Police);
- The covert surveillance must cease as soon as the investigation is complete.

8 Access to CCTV Materials

The Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002 will be adhered to. Any request for disclosure of information must be made in writing to the University's Data Protection Officer [dpa@abdn.ac.uk].

Live footage must be monitored in a self-contained and secure area. Remote access to live images must be approved in advance by the University Secretary in consultation with the relevant Head of School and the Director of Estates.

Only appropriately trained designated staff and their management shall have direct access to live or recorded CCTV footage. Other requests to access CCTV footage including from the subject of the image, should be dealt with in writing to the University's Data Protection Officer [dpa@abdn.ac.uk].

The University will only investigate images for use in a staff disciplinary case when there is a suspicion of gross misconduct. CCTV will not be used to generally monitor staff activity. In these situations the Investigating Manager or HR Partner/Advisor will formally request access to images in terms of the Policy for Access to Personal Data approved by the University Court on 28 June 2011. Where access is given, the confidentiality of these images and who is able to access them will be closely controlled as described in Appendices 2 and 3 and Paragraph 5.2.2 of the ICO Code of Practice.

Disclosure of images to third parties is limited to the following:

- Police;
- Other law enforcement agencies;
- Prosecution agencies;
- Relevant legal representatives;
- University management with a legitimate reason for accessing images e.g. investigating potential gross misconduct of staff or students.

There must be an audit trail to show who has accessed recorded footage in order to satisfy any investigation by the ICO.

Recorded data will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.

9 Staff Training

Designated staff and anyone else with access to a CCTV room or CCTV recordings must receive appropriate training in the operation of the system, the legal requirements associated with its use, and any other relevant procedures and policies.

10 System Maintenance

An appropriate maintenance programme must be established and implemented for all systems. This must include arrangements for prompt fault identification and repair.

11 Retention and Disposal of Recorded Materials

CCTV recordings and other materials produced from the CCTV recordings shall normally be retained for a minimum of 21 days before being erased. If an incident is recorded that could give rise to claims against the University, these recordings must be kept for a period of 6 years from the date of recording.

Footage produced as part of a criminal, civil or disciplinary case will be retained for a minimum of 6 months after closure of the case.

Hard drives and other media must be destroyed securely as confidential waste.

Metadata			
Title	CCTV Policy		
Author / Creator	Stanley Jack (Estates)		
Owner	University Management Group		
Date published / approved	27 June 2017		
Version	Draft (v1.0) Approved (v1.1) Approved (v1.1a) Approved (v1.1b)	Jun ‘16 20 Feb ‘17 17 May ‘17 27 Jun ‘17	AGED for EIA UMG PNCC Court
Date for next review	2018		
Audience	All		
Related Documents	Data Protection Act 1998 Freedom of Information (Scotland) Act 2002 ICO Code of Practice for Surveillance Cameras and Personal Information (2015)		
Subject / Description	A policy statement outlining the principles for the University’s installation and operation of closed circuit television (CCTV) and associated remote surveillance systems.		
Equality Impact Assessment	EIA completed (6 June 2016)		
Section	Estates		
Theme	Campus Security, Information Security		