POLICY NAME:	**CCTV, Surveillance and Access Control Systems Policy**
Policy Category:	General
Subject:	CCTV, Surveillance and Access Technology use and management
Approving Authority:	Senior Management Team
Responsible Officer:	Principal
Responsible Office:	Estates and Facilities Operational Assurance
Related Procedures:	CCTV, Surveillance and Access Control Systems Procedure Requests for Personal Information Procedure Data Breach Management Procedure
Related College Policies:	Information Security Policy Data Protection Policy
Effective Date:	5 December 2019
Supersedes:	March 2016
Next Review:	31 July 2023

---

1. Purpose & Scope

1.1 This policy sets out the accepted use and management of video surveillance systems or any other surveillance technology including CCTV and access control systems to ensure the university complies with its legal obligations and respect for individual privacy of its students, staff, contractors and visitors.

1.2 This policy covers the use of surveillance technologies including CCTV and access control systems which record personal data relating to individuals on university premises, where the university is the controller of the data. The policy also covers technology which monitors space to support more efficient building management, space and energy use. The policy is designed to be compliant with the university data protection procedure.

1.3 This policy has been designed to ensure that the practices adopted by the university are consistent with the Information Commissioner's (ICO) CCTV Code of Practice 2017.

2. Definitions

2.1 CCTV is defined as fixed cameras designed to capture and record images of individuals.

2.2 Surveillance System is defined as any electronic system or device that captures images of individuals or information relating to individuals. This term is used in this policy to refer to any surveillance technology including CCTV. It includes any technology that may be introduced in the future for a similar purpose such as automatic number plate recognition (ANPR), body worn cameras or aerial surveillance.

2.3 Access control system is the physical access management to buildings and offices through swipe ID cards.

2.4 Building monitoring technology is defined as equipment which provides aggregated and anonymised data on the occupation of university space.

2.5 Systems data is defined as any personal data held or captured by a video surveillance or access control system.

2.6 Security Systems Technicians are employees of the university, working within the Estates & Facilities Directorate, to maintain the door and controller hardware associated with the CCTV, security and access control systems.

2.7 Staff is defined as those individuals employed directly by the university.

2.8 Contractors are defined as employees of companies contracted to supply a service to the university.

3. Roles and Responsibilities

3.1 The Estates and Facilities Directorate is responsible for the management of the systems.

4. Policy

Operation of the systems

4.1 The university uses video surveillance and door access systems to provide a safe and secure environment for students, staff and visitors, and to protect university property.

4.2 The university will decide where to install video surveillance technology based on a Threat and Security Risk Assessment conforming to British and European standards.

4.3 Where new technologies are considered for use as video surveillance systems, these should be subject to a Data Protection Impact Assessment (DPIA or PIA) in accordance with the ICO Code of Practice on Privacy Impact Assessment.

4.4 Video surveillance and door access systems operate continually.

4.5 CCTV signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV or surveillance installation is in use.

4.6 The systems will be provided and operated in a way that is consistent with an individual's right to privacy, and other rights under all applicable data protection and privacy legislation.

Digital Images

4.7 If images show a recognisable person, they are personal data and are covered by the applicable UK data protection legislation. The university's Data Protection Policy must be adhered to at all times.

Processing Data

4.8 The university maintains a Record of Processing Activities (ROPA) register, identifying activities that include processing of personal data (including images). CCTV image capture and access control data are included on the Estates & Facilities' ROPA.

4.9 The university has the right to use data captured by the system for all reasonable operational or investigative purposes, as outlined in the procedure accompanying this policy. Access to the data will be controlled by nominated authorisers.

4.10 Data derived from building management monitoring technology will not be used to identify any individual or group, where group size is so small as to allow individual behaviour to be inferred, or to indicate the specific use of space by an individual or group, where group size is so small as to allow individual behaviour to be inferred.

Individual Access Rights

4.11 Anyone who believes their personal data (either image or access information) has been captured by one of the systems can request a copy of that data subject to the considerations of the relevant data protection legislation.

4.12 Requests should be made using the Subject Access Request process of the university and should include all information necessary to locate the images or information on the recording system. The list of required information is contained in the CCTV Procedures. Data subjects can also exercise their other Data Subject Rights through this same process.

Access by Third Parties

4.13 Access to images and door access information will be restricted to those staff and contractors that need to have access in accordance with the purposes of the system, to undertake their legitimate duties or to discharge their responsibility towards the university.

4.14 Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and the prevailing data protection legislation, other relevant legislation and considering individual data protection rights.

4.15 All third-party requests for access to a system data footage should be made in writing to the Information Compliance team. If a law enforcement or prosecution agency is requesting access, they should make a request under the relevant Data Protection legislation.

4.16 From time-to-time contractors working on systems will require access to system data. Where this information relates to personally identifiable data, the data release will either be anonymised or covered by a formal data-sharing agreement.

Retention

4.17 The university operates a retention schedule which must be adhered to and will dictate the period of retention for all data held by the CCTV and access control systems.

Covert Monitoring

4.18 Covert monitoring (where the individual is not aware the monitoring is taking place) will only be justifiable in exceptional circumstances where there are grounds to suspect criminal activity or extremely serious malpractice. If such monitoring is undertaken:

- A lawful basis for processing is identified
- It must be with the prior authorisation of the Directorate of Estates and Facilities' Director of Operations or the Director of Estates & Facilities and the Senior Vice President (Operations);
- The decision to undertake covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom;
- It will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity;
- The risk of intrusion on innocent parties is considered;
- Areas where a high level of privacy is expected remain private;
- Only limited numbers of people will be involved in the monitoring.

5. Review and monitoring

5.1 The policy will be reviewed every three years or when legislation updates occur.