|  |  |
| --- | --- |
|  | CCTV (and video surveillance) policy |
|  | Author: Colin Montgomery  Review: Every 3 years, or as required   |  |  |  | | --- | --- | --- | | Date | Version | Update | | 11 April 2025 | Version 1.0 | Major redraft from previous Code of Practice | |
| April 2025 |  |
|  |  |

# Introduction

The University of Strathclyde uses video surveillance equipment within its business premises and the external areas of the University campus. The main systems used are closed circuit television (CCTV) systems. However, for the purposes of this policy, the term ‘CCTV’ should be understood to include other ‘video surveillance’ or other image recording systems the University may employ for the same purposes (as set out below), e.g. Automatic Number Plate Recognition (ANPR).

The University aims to operate CCTV in a proportionate manner, which considers the privacy rights of individuals. Recorded CCTV images of identifiable individuals are personal data and must be processed in accordance with data protection legislation and the University’s Data Protection Policy. This policy outlines how the University employs CCTV and how it meets its legal obligations.

# PUrposes

The CCTV system will be used for the following purposes:

* to reduce the fear of crime and to reassure the University community and the wider public.
* to detect, prevent or reduce the incidence of crime and anti-social behaviour.
* to prevent and respond to any incidents which may affect the safety and security of the University community and the University estate.
* to assist in the protection and management of university assets, facilities, or estate, including traffic management/car parking; and
* to assist with the investigation of university regulations, policies and procedures.

Any CCTV or video surveillance system used anywhere on the University campus which is used for these purposes is covered by this policy. Associated purposes for the use of CCTV may apply, depending on the specific circumstances, e.g. defending the University against claims made against it. These will be considered on a case-by-case basis, to ensure consistency with this policy and applicable legislation.

# SCOPE

The policy applies to all CCTV systems, equipment and images managed by or on behalf of the University on its estate for the purposes set out above.

The University estate includes the main University campus (the John Anderson campus), and any satellite locations, e.g.: National Manufacturing Institute Scotland (NMIS); Power Network Distribution Centre (PNDC); Advanced Forming Research Centre (AFRC); and Stepps playing fields.

The policy applies to all staff, contractors and any other individuals authorised by the University to manage, maintain, support or view CCTV systems, equipment and/or images. It is also relevant to staff, students, contractors, visitors and members of the public who may be recorded on CCTV.

# roles and responsibilities

**The Head of Security Services**

* has overall responsibility for the production and review of this policy.
* is responsible for the management and operation of all CCTV systems under the control of Security Services and compliance with the policy in relation to these systems*.*
* ensuring appropriate training of Security Services staff*;* and
* must be consulted in advance regarding the installation of any new CCTV equipment/ systems within the scope of this policy.

**Security Supervisors**

* will undertake regular checks to ensure procedural compliance, e.g. on a weekly basis.
* will conduct and record regular audits into the operation of the system; and
* direct staff to complete training, where appropriate.

**Security Services staff and any other staff/individuals who operate, manage or process images from CCTV systems**

* must be aware of all relevant policies, procedures, guidance and codes of practice.
* must act in accordance with this policy; and
* must undertake relevant training as instructed.

**CCTV not managed by Security Services**

In some locations CCTV is not managed by Security Services, e.g. in some satellite locations. In such locations, the most senior member of staff or delegate (with responsibility for CCTV) must ensure that:

* appropriate contractual clauses are in place with any organisations providing services to the University relating to CCTV and they are made aware of this policy and the requirement to comply with it.
* an appropriate individual is delegated authority to manage CCTV on a day-to-day basis; and
* appropriate staffing is in place to manage CCTV, and adequate training is provided to those staff in relation to their obligations,

in accordance with this policy.

**Service providers/contractors**

Third parties who are engaged by the University to provide services which include the use of CCTV must:

* be aware of and comply with this policy.
* make sure that their staff are aware of their obligations, are adequately trained and made aware of this policy; and
* otherwise only act in accordance with their contractual obligations.

**Information Governance Unit**

* is responsible for responding to all requests from individuals relating to their rights under data protection legislation.

# SYSTEM and operation

**Management and maintenance**

* CCTV system and equipment must be checked and maintained regularly to ensure that it functions adequately and is fit for purpose.
* Images must be clear enough to meet the University’s stated purposes.

**Location and Operation**

* The system comprises internal cameras within University buildings monitoring both public and secure areas.
* There are also cameras covering external areas of University premises, including “streetscape” cameras covering the John Anderson Campus.
* Cameras are positioned in a manner that recognises the security risks associated with each specific location; surveillance should not occur in areas where no security risk has been identified.
* Cameras do not record sound.
* CCTV does not include areas where there is an expectation of increased privacy, e.g. changing rooms or toilet areas.
* Only suitably trained staff are authorised to operate the equipment.
* Misuse of surveillance system information will be considered under relevant disciplinary processes and could be a criminal offence.
* CCTV under the control of the University’s Security Services team is centrally controlled and monitored on the John Anderson Campus; data is stored on University of Strathclyde servers.
* CCTV systems which do not fall under the remit of University’s Security Services team should be managed in line with this policy.
* Any additional/increased use of CCTV must be discussed with the Head of Security Services in advance. Privacy risks must be considered/addressed in advance through appropriate data protection assessments.
* Covert recording is not standard practice in the University. Any such request must be based on substantial evidence of the need and intended benefit. A request to undertake covert recording must be discussed with the Head of Security Services, Data Protection Officer and relevant senior officers in the University in advance. Relevant legislation, guidance and codes of practice must be considered.

**Access and System Security**

* Access to CCTV control rooms is limited and audited.
* Only authorised individuals will be permitted to view images, this can include technical staff and contractors responsible for system maintenance and repair.
* Each team member operating a CCTV system will have their own log in credentials to access the system and its data.
* Authorisation to view images may be extended to other staff out with Security Services/staff who directly manage and operate CCTV systems, e.g. staff charged with internal investigations or managing requests made under legislative rights/powers.
* Viewing/reviewing of any images must be undertaken in a secure area, out with the view of unauthorised individuals.
* Any images downloaded and or produced from the system must be managed, transmitted and stored in a way that ensures the ongoing integrity, availability and confidentiality of those images.
* Data shall, always, be protected by appropriate technical measures.
* Internal requests for access to CCTV images shall be directed to the Head of Security.

## Signage and transparency

The University must alert individuals to the operation of CCTV. This includes the provision of signage alerting individuals to the operation of CCTV where cameras are recording and relevant details about the system operator. Further information about the use of CCTV is provided in this policy and in applicable CCTV privacy notices.

# Disclosure of CCTV IMAGES

**Subject Access Requests**

Individuals have a right under data protection legislation to request access to their own personal data (a Subject Access Request). This can include CCTV images. Any Subject Access Requests should be forwarded to the Information Governance [dataprotection@strath.ac.uk](mailto:dataprotection@strath.ac.uk)

**Third party requests**

Requests for access to CCTV images may be made by third parties, including the police. Disclosure of recorded images to third parties will be controlled and consistent with the purpose for which the system was established. Generally, requests will be made in writing citing the relevant legislation, often using a standard form. Responding to such requests will require input from Security Services and may also require input from colleagues in other areas of the University, including the Information Governance Unit.

If any type of request from a third party in relation to CCTV is received, then this will be dealt with on a case-by-case basis, in line with this policy and any other applicable legislation.

Where the request is an ‘emergency’ and ‘time is of the essence’ the relevant member of Security Services staff will judge whether to provide the information without the submission of an appropriate form in advance/at the time of the request. Providing access to images to the police without a completed standard form should be considered to be ‘exceptional’ and not the University’s standard practice, by either staff or law enforcement agencies. It is recommended that even where disclosure is made without submission of a form in advance, that one is submitted subsequently.

**Legal obligations**

If the University is legally required to disclose images, then this will be managed by the appropriate team, in collaboration with Security Services/the individual with responsibility for the CCTV system. All Court Orders are managed by Legal Services.

**Other third-party requests**

Any other third-party requests for access to CCTV will be considered and assessed in line with the purposes for which the images were recorded. Where the disclosure is for a purpose other than those stated in this policy and where there is no legal obligation for the University to provide the information e.g. insurance claims, disclosure is at the discretion of the University.

# Retention and Disposal

In general, recorded CCTV images are automatically deleted after 14 days. Some project-specific CCTV data is routinely retained for 30 days.

Where an incident has led to or is considered likely to lead to further investigation, either internally or externally, relevant images will be downloaded. In normal circumstances copies will be erased after 3 months if no further request is made for them, from the date of download.

Any images downloaded from the CCTV system must be stored securely until deleted. Images must be securely disposed of, irrespective of the media on which they are stored.



# Data Protection

Under data protection legislation, the University is the Controller for all images recorded by CCTV equipment managed by or on behalf of the University. The University is therefore responsible for ensuring that CCTV images are processed in accordance with: data protection legislation; relevant guidance produced by the Information Commissioner’s Office; and the [University’s Data Protection Policy](https://www.strath.ac.uk/whystrathclyde/universitygovernance/accesstoinformation/dataprotection/yourrights/). Additional information can be found in the CCTV Privacy Notice, which is published on the University website.

**Data Subject Rights**

Under data protection legislation, individuals have several rights, including the right to request access to their own personal data. The Information Governance Unit (IGU) will process any subject rights request, including requests relating to CCTV footage, in conjunction with Security Services.

# Compliance

All staff dealing with CCTV equipment and recordings should be aware of this CCTV Policy and any other relevant policies, procedures, guidance and codes of practice. In addition, these staff members should receive appropriate training to ensure they are aware of the correct operation of the system and handling of personal data.

Any misuse of information obtained from a video recording is a serious issue and may result in disciplinary action being taken against the member of staff involved. It may also be a breach of data protection legislation and could also be a criminal offence.

# Policy Review

The Head of Security Services will ensure that a formal review of the University’s CCTV system, including associated policies, procedures and documentation is carried out every three years or as otherwise required.

There will be several forms associated with the management of CCTV. These may be amended and updated independently to this policy, unless the change/amendment constitutes a change of this policy.