Security & Campus Safety CCTV Code of Practice Policy

Next Review Date: February 2022 **Estates & Campus Services** **University of Essex**

VERSION CONTROL

VERSION	COMMENTS	DATE	UPDATED
0	Draft Copy Made, Consultations, review and feedback	01/03/2020	TB
1	Submitted for approval by USG	Feb 2021	TB

AUTHORISED BY:

Name	Role	Date
Chris Oldham	**Director of Estates & Campus Services**	**01/02/2021**
Tim Morris	**Deputy Director of Estates & Campus Services**	**01/02/2021**

RESPONSIBLE PERSONS:

Name	Role
Thomas Brown	**Head of Security & Campus Safety**
Marc Lee	**Deputy Head of Security & Campus Safety**
Sara Stock	**University Data Protection Officer**

Any amendments or suggested alterations should be sent to the Head of Security & Campus Safety, University of Essex, Wivenhoe Park, Colchester, Essex, CO3 4SQ. Tel: 01206 872361.

CONTENTS

Definitions 4
Section 1 - Scope 5
Section 2 - Ownership 5
Section 2.1 - Responsible Person Contact Details: 5
Section 2.2 - General Enquires 5
Section 2.3 - Responsibilities 5
Section 2.4 - Installation 6
Section 2.5 - Monitoring and Evaluation 6
Section 3 - Introductions 6
Section 3.1 - Principles 7
Section 3.2 - Key Aims and Objectives for the System 8
Section 3.3 – Health and Safety Breaches 8
Section 4 - Complaints 8
Section 4.1 - Breaches of the Code of Practice 9
Section 5 - Data Protection Act 2018 / General Data Protection Regulation 2018 9
Section 6 - CCTV System 9
Section 6.1 - Maintenance of the System 10
Section 6.2 - Body Worn Cameras 10
Section 7 - Control Room Administration and Procedures 10
Section 7.1 - Staff 11
Section 7.2 - Data Handling Procedures 11
Section 7.3 – Recording and still images 12
Section 7.4 - Digital Recording Procedure 13
Section 7.5 - Police Service and assistance 13
Section 8 - Access to Recordings and Disclosure 13
Section 8.1 - Standards 14
Section 8.2 - Access by Data Subjects 15
Section 8.3 - Rights of Data Subjects 15
Section 9 – Support Documents 16
Appendix 1: How to Apply For Access to CCTV External 16
Your Rights 17
The University Rights 17

The Application Form: 17
Appendix 2: Request for Viewing/Extract of Footage (Internal Only) 21
Appendix 3: Disclosure of Data to Persons Other Than the Police 22

DEFINITIONS

For this Code of Practice, the following definitions will apply:

'System' - The University of Essex CCTV comprising of body worn CCTV

'Control Room' – Control Rooms at Colchester & Southend Includes Loughton Campuses

'His / Her Nominee' - This can be the Deputy Head of Security & Campus Safety, Duty Security Manager (Colchester), Security Co-Ordinator (Southend & Loughton), Security Supervisors or Data Protection Officer.

SECTION 1 - SCOPE

This Code of Practice is binding on all staff, students, contractors, and visitors or members of the public to the campuses, and apply to all other persons who may, from time to time, and for whatever purpose, be present on University property.

SECTION 2 - OWNERSHIP

The University of Essex owns the CCTV system which operates across all campus' property. All recorded material is owned by, and the copyright of any material is vested in, the University. It is the University responsibility to ensure the compliance with this Code of Practice, its responsibilities under the relevant legislation, regulatory requirements and statutory obligations and to approve and ensure compliance with the operating procedures for the System. It is also the University's responsibility to notify persons entering areas monitored by the System that a CCTV system is in operation and where required audio is in operation, to provide copies of this Code of Practice when requested to do so. The University of Essex Security & Campus Safety Team, whose personnel are employed directly by the University, operate the system together with third parties who may operate the system on behalf of the University.

SECTION 2.1 - RESPONSIBLE PERSON CONTACT DETAILS:

Primary Contact:

- Title: Head of Security & Campus Safety and where required his/her nominee
- Organisation: University of Essex
- Email: securitymanagement@essex.ac.uk
- Telephone: 01206 872125
- Address: Wivenhoe Park, Colchester CO4 3SQ

Secondary Contact:

- Title: Data Protection Officer
- Organisation: University of Essex
- Email: dataprotectionofficer@essex.ac.uk
- Address: Wivenhoe Park, Colchester CO4 3SQ

SECTION 2.2 - GENERAL ENQUIRES

Any enquires concerning this Code of Practice and/or the operation of the System should be directed to the Head of Security & Campus Safety.

SECTION 2.3 - RESPONSIBILITIES

It is the responsibility of the Head of Security & Campus Safety or in their absence, his / her nominee to:

- Have in place a system whereby cameras are only sighted in locations that show a pressing need for surveillance in accordance with the aims and objectives.
- Ensure the CCTV system and Body Worn complies with the data protection and other legislation

- Manage the process of image and data retention, security and viewing by authorised persons
- Regularly evaluate the system to ensure it complies with the latest legislation, Codes of Practice and offers the best value to the University.

SECTION 2.4 - INSTALLATION

- No installation or additional cameras can be added or installed on the University campuses without consultation with the Head of Security & Campus Safety or his / her nominee.
- Any installation connected with the system will be appropriate to its purposes and the requirements of this Code of Practice.
- When installing cameras that may overlook any residential accommodation, the University will have regard for the privacy of any residents this will include any masking of windows, should CCTV overview these areas.

SECTION 2.5 - MONITORING AND EVALUATION

- This Code of Practice, the operation of the University system will be reviewed annually by the Head of Security & Campus Safety or a nominated person.

SECTION 3 - INTRODUCTIONS

The University has installed a comprehensive CCTV surveillance system, which is across the University. Cameras have been installed in all key areas of our campuses including teaching, outdoor spaces, accommodations, car parks, licensed premises and sensitive areas. These are monitored at one of our two control rooms located at Colchester or Southend which covers both Southend and Loughton.

The University owns and operates a various range of cameras across the University with fully functioning Pan Tilt and Zoom (PTZ) facilities, fixed cameras with audio and body-worn CCTV with audio. Body worn CCTV is also used by members of staff to ensure a secure and safe environment for operators during their duties to tackle abuse, violence and anti-social behaviour.

This Code of Practice has been prepared for the guidance of management, the operators of the CCTV system and to inform all members of the University community and those using University facilities at any time. Its purpose is to ensure that the CCTV system is used to create a safer environment for staff, students, contractors, visitors and members of the public to the University, consistent with the obligations on the University imposed by the Data Protection Act 2018, General Data Protection Regulation (GDPR) (and associated regulations), the Protection of Freedoms Act 2012 and other legislative and statutory obligations.

The Information Commissioner's Office (ICO) issued code of practice and guidance, now under the Data Protection Act 2018 (DPA), covering the use of CCTV. The code had been developed to explain the legal requirements that operators of surveillance cameras were required to meet under legislation and promote best practice. The code also addressed the inconsistent standards adopted across different sectors at that time and the growing public concern caused by the increasing use of CCTV and other types of surveillance cameras.

The increased use of CCTV and other forms of surveillance cameras and equipment led to a strengthening of the regulatory landscape through the passing of the Protection of Freedoms Act 2012 (POFA). POFA introduced a new surveillance camera code made by the Surveillance Camera Commissioner to promote the code and review its operation and impact on the public.

The Information Commissioner's Office has contributed to this tougher regulatory landscape by taking enforcement action to restrict the unwarranted and excessive use of increasingly powerful and affordable surveillance technologies. It does mean that the University which operates a CCTV System is required to comply with these procedures and requirements.

The University's Head of Security & Campus Safety retains overall responsibility for the system on behalf of the University and delegates the day to day management to the Duty Security Management Teams and Supervisors. It is their responsibility to ensure that CCTV within the University is managed in line with this Code of Practice, the current CCTV Code of Practice produced by the Information Commissioner's Office, the current Surveillance Camera Code of Practice issued by the Surveillance Camera Commissioner and data protection legislation.

- All images produced by the system remain the property and copyright of the University.
- The University will only investigate images for use in a staff or student disciplinary case when there is a suspicion of misconduct and not to generally monitor staff activity and performance. In these situations, it will be requested from the investigating manager via the Human Resources who will formally request access to images on their behalf to the Head of Security & Campus Safety or his / her nominee, where these may prove or disprove suspected potential misconduct / gross misconduct. Where access is given, the confidentiality and security of these images and who can access them will be closely controlled and any stored or saved images will remain in the Security Virtual Locker. A review date is set within this document of 31 days and a maximum of 90 days, it will be down to the Head of Security & Campus Safety or his / her nominee for any extensions required to holding the recordings.
- The University Security & Campus Safety Service Control Rooms and reception areas contain CCTV and audio and these may be periodically checked by the Senior Management Team for any complaints, investigations, operational reviews, monitoring of incidents or CCTV operators' performance in line with this Code, Human Resources Guidance and with a valid given reason for the review or monitoring made to the Head of Security & Campus Safety or his / her nominee before a review takes place.

The objectives outlined in this Code will be closely followed when assessing the requirements for new CCTV installations. Similarly, if designated usage of the area changes it will be necessary to assess whether the location of cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation.

SECTION 3.1 - PRINCIPLES

The following principles will govern the operation of the CCTV monitoring System:

- The CCTV monitoring System will be operated fairly and lawfully and only for the purposes identified by the University of Essex.
- The System will be operated with due regard for the privacy of the individuals whose images have been captured.
- Any change to the purposes for which the system is operated will require the prior approval of University in advance.

- To ensure the security and integrity of the University Security operating procedures, these will be implemented and amended only with the prior consent of the Head of Security & Campus Safety, Data Protection Officer or his/her nominee

SECTION 3.2 - KEY AIMS AND OBJECTIVES FOR THE SYSTEM

The CCTV installed across the University Campuses is to reduce the fear and impact of crime across all of the campuses and to provide a safe public environment for the benefit of those who live or work in, or who visit the University. These objectives and aims will be achieved by the monitoring of the system:

- To prevent, detect and reduce the incidents of criminal activity at the University.
- To facilitate the identification, apprehension and prosecution of offenders concerning crime and public disorder; and as an aid to public safety.
- To detect, prevent and reduce offences against the person or property.
- To improve the efficiency with which the University can alert the Police to any unlawful activity.
- To assist in the University Emergency procedures and Operations
- To assist with Civil Emergencies that take place
- To provide the Police, Emergency Services, HM Customs and Excise, Health and Safety Executive, and University with evidence upon which to take criminal, civil and disciplinary action respectively.
- To support crowd Management and Public Safety for any events taking place on our campuses
- To prevent and enable the University to respond effectively to any harassment and bullying.
- To assist with traffic management operations, such as the provision of University parking facilities and the lawful use of these facilities.
- To provide a Training facility for new Staff or internal SIA training courses and provide footage for training purposes
- To assist in safeguarding the health and safety of staff, student contractors, visitors or members of the public.

SECTION 3.3 – HEALTH AND SAFETY BREACHES

It should be noted that any intentional or reckless interference with any part of the system (including cameras) may constitute a criminal offence and will be regarded as a breach of discipline.

SECTION 4 - COMPLAINTS

The University operates a complaints procedure which can be found on the University website to raise any concerns if members of staff, students, contractors, visitors and members of the public, whose images are captured on the systems, have concerns or questions about the use of the CCTV in place.

University Complaint Link:
https://www1.essex.ac.uk/records_management/help/complaints.aspx

Any enquiries should be directed to the Head of Security & Campus Safety, or nominee on the details above. The system is registered with the Information Commissioners Office (ICO)

and can only be used under those registered aims and objectives as deemed by the University Data Controller. These are contained in this Code.

SECTION 4.1 - BREACHES OF THE CODE OF PRACTICE

The University reserves the right to take disciplinary action against any employee, student, contractor or user of University premises, who breaches this Code of Practice.

SECTION 5 - DATA PROTECTION ACT 2018 / GENERAL DATA PROTECTION REGULATION 2018

In compliance with its data protection obligations in accordance with the data protection legislation and its role as a Data Controller:

- The recorded material shall be obtained and be processed fairly, lawfully and following this Code of Practice and in accordance with the University's Data Protection Policy.
- The recorded material shall be processed for the purposes outlined in this Code of Practice.
- The recorded material shall not be used or disclosed for any purpose, or in any manner, which is incompatible with this Code of Practice.
- The recorded material shall be adequate, relevant and not excessive concerning the purposes set out in this Code of Practice.
- Where recorded material is retained for any of the purposes set out in this Code of Practice, that material shall not be kept for longer than is necessary for the purpose for which it is being retained and shall be stored in a secure manner requiring authorised access.
- Access to the recorded material will be permitted strictly under this Code of Practice and the operating procedures detailed for the Security & Campus Safety Services.
- The legal basis for processing under data protection legislation are vital interests of the data subject ; processing carried out in the public interest ; and the legitimate interests of the Data Controller

The University will ensure that appropriate security measures are taken to prevent unauthorised access to, the alteration of, disclosure or unlawful destruction of any recorded material; and to prevent accidental loss or destruction of such material. Recorded material will not be sold, used for commercial purposes, used for the provision of entertainment or used to provide information or material for research purposes.

SECTION 6 - CCTV SYSTEM

The University of Essex systems consist of:

- Overt Pan, Tilt, Zoom (PTZ) and static cameras – covering areas around the campuses property.
- Body Worn CCTV – used by security when on patrol and during all periods of the day to help deal with incidents that they attend and support with evidence gathering during drunk and disorder, violence, anti-social behaviour and any other incidents deemed relevant to the use of the body-worn camera to protect the officers and people involved..

Given that CCTV cameras cover a wide area of the University Campuses and areas to which members of the public has access, every effort will be made to inform the staff, students, contractors, visitors and members of the public by way of signs at regular intervals and the entrance zone of areas covered by cameras.

Signs will be placed at the entrance to the CCTV zone to inform the public of the presence of the system and its ownership in line with the ICO requirements. Clear and prominent signs are particularly important where the cameras themselves are discreet or are in locations where people might not expect to be under surveillance.

Images captured on camera will be transmitted either to the Control Room or to separate stand-alone systems where they will be recorded for use under this Code of Practice. Although every effort has been made in the planning and design of the CCTV system to deliver maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

SECTION 6.1 - MAINTENANCE OF THE SYSTEM

To comply with the relevant data protection legislation the CCTV systems will be maintained efficiently and effectively, ensuring images comply with the quality standards expected under the legislation. A maintenance agreement is in place setting out the terms of how the system will be maintained and improved all maintenance jobs will be logged directly to the engineer to attend.

Emergency attendance by engineers is part of the maintenance agreement and any faults will be rectified without delay. This is to ensure a service is provided to the staff, students, contractors, visitors and members of the public within the CCTV areas.

SECTION 6.2 - BODY WORN CAMERAS

Body Worn CCTV is used by security when on patrol and images are required to provide evidence of offences or another behaviour that might require action by security. Persons subject to the recording by Body Worn CCTV will be made aware that it is in use by the security officer making a verbal announcement unless circumstances prevent that from happening.

The recording will only take place when there is a valid reason for doing so. Images that are recorded will be managed under this Code of Practice, the Body-Worn Camera Policy and our obligations under data protection legislation..

SECTION 7 - CONTROL ROOM ADMINISTRATION AND PROCEDURES

An incident log will be maintained in the Control Rooms and details of incidents will be noted together with any consequential action taken. All copies will be handled under the procedures outlined in this Code and are designed to ensure the integrity of the system. The Head of Security & Campus Safety or his / her Nominee will be responsible for the development of and compliance with the working procedures in the Control Room.

Due to the sensitive nature of the control room in the tasks and duties that are required to carry out and incident management perspective. The control room itself is monitored with visual and audio. This may be reviewed for any complaints, investigations, operational reviews, monitoring of incidents or CCTV operators performance in line with this code, Human Resources guidance and with a valid given reason for the review or monitoring made to the Head of Security & Campus Safety or his / her nominee before a review takes place There

are further details set out above for the usage of them recording and in the local SOP documentation.

Recorded images will only be reviewed with the authority of the Head of Security & Campus Safety or his / her nominee. Copies of recorded or digital images will only be made for the purposes of the aims and objectives within this Code of Practice and sections.

SECTION 7.1 - STAFF

All staff involved in the operation of the CCTV system will, by training and access to this Code of Practice, be made aware of the sensitivity of handling CCTV images and recordings.

The Head of Security & Campus Safety or his / her nominee will ensure that all staff, including relief staff, are fully briefed and trained in respect of all functions, both operational and administrative, arising within the CCTV control operation. Agency Security Officers who use the system will be trained via the Security Industry Public Space CCTV Licence this is not relating to use of Body Worn CCTV and that Policy should be consulted.

All staff are trained in current legislation as it applies to CCTV taking into account: -

•The Data Protection Act 2018, The General Data Protection Regulation and associated legislation

• The Human Rights Act 1998

• The Protection of Freedoms Act 2012

• The Freedom of Information Act 2000

• The Regulation of Investigatory Powers Act 2000

In addition, all staff are trained in the effective operation of CCTV equipment and processes to comply with this Code of Practice and current legislation. CCTV operators do require a Security Industry Authority licence to use and operate the system unless they are in-house security however it will be expected of them being trained to a similar standard. On some of our campuses, our Security Patrol Officers will be Security Industry Licences in Public Space CCTV.

SECTION 7.2 - DATA HANDLING PROCEDURES

- Images captured by the system will be monitored in the Control Rooms. The Control Rooms are self-contained, and the monitors cannot be seen from outside of these rooms.
- No unauthorised access to the Control Rooms is allowed at any time. Normal access is strictly limited to the Security & Campus Safety Services. Police officers may enter with the explicit consent of the Head of Security & Campus Safety or his / her nominee.
- Persons other than those specified in the above may be authorised to enter the Control Room on a case-by-case basis. Written authorisation is required and may only be given by the Head of Security & Campus Safety or his / her nominee. Each separate visit will require individual authorisation and will be supervised, always, by the Head of Security & Campus Safety or his / her nominee. Such visitors will not be able to access view any data, which falls within the scope of the data protection legislation.

- In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter the Control Rooms.
- Before granting access to the Control Rooms, operators must satisfy themselves of the identity of any visitor and ensure that the visitor has the appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or the organisation they represent, the person who granted authorisation for their visit (if applicable) and the times of their entry to and exit from the Control Rooms. A similar record shall be kept of the operators of the CCTV systems whilst on duty in the Control Rooms at any given time.

SECTION 7.3 – RECORDING AND STILL IMAGES

- The Control Room system is a digital recording system, which can retrieve images to a digital system.
- Images are recorded digitally; the process of identifying retrieval dates and times is computerised. Images will be cleared automatically after a set time on the system.
- Unless required for evidential purposes or the investigation of crime, recorded images held on the CCTV system will be retained for no longer than 31 days from the date of recording as per the system capacity. However, the University recognises that, under the requirements of GDPR and the Data Protection Act 2018, no images should be retained for longer than is necessary. Accordingly, some recorded images may be erased after a shorter period, for example, where it can be determined more quickly that there has been no incident giving rise to the need to retain the recorded stored images.
- The use of Discs, USB or secure share platform from the CCTV system may be used to share images or recordings for investigations. These will be held securely within the University and logged on a tracker when released.
- Recordings of Body Worn CCTV will be retained for 31 days unless deemed evidential and will be held on the virtual locker for 1 year.
- In the event of the digitally recorded image being required for evidence or the investigation of crime, it will be retained for a period until it is no longer required for evidential purposes or any investigation into a crime has been completed and will be reviewed periodically by the Head of Security & Campus Safety or his / her nominee.
- Still, photographs will be generated from recordings made by the system only where these are required for evidential purposes by the Police or other bodies with prosecuting powers, or by the University.
- Unless required to do so by a court of law, recordings made by the system and/or still images generated from such recordings will not normally be made available by the University to individuals wishing to use them as evidence in any civil litigation.

The University reserves the right to use a recording made by the system and/or still images generated from such recordings, as evidence in internal grievance/complaints investigations and/or in disciplinary investigations involving staff, students or contractors of the University. The University reserves the right to use a recording made by the system and/or still images generated from such recordings, in any civil prosecution brought by the University.

SECTION 7.4 - DIGITAL RECORDING PROCEDURE

All discs and USBs belong to and remain the property of University. Disc or USB handling procedures are in place to ensure the integrity of the image information held and a timescale is set out above under the recording section.

All computer disks containing CCTV images, or any still photograph or printed image, shall be marked with a unique number. A log will be maintained within the Control Rooms and managed by the Head of Security & Campus Safety or his / her nominee. This will contain details as to the dates when the disk/photograph/print was introduced into the system or created and when it was disposed of. An entry will be made in the log of any dates the disk/photograph/print was removed from the control room, together with the identity of the person removing it and the reason for such removal.

SECTION 7.5 - POLICE SERVICE AND ASSISTANCE

Whilst the CCTV system always remains under the control of the University, when a request is received from agencies with a law enforcement role for assistance, any such assistance will only be given in accordance with the law and after due consideration by the Head of Security & Campus Safety or His / Her nominee who will reserve the right to refuse assistance if it is deemed unlawful or not appropriate to the aims and objectives of the System.

On each occasion the Police obtain assistance with their operations a report setting out the time, date and detail of the incident will be submitted to the Head of Security & Campus Safety or His / Her nominee. Details of such incidents will be recorded on the Incident reporting log with a relevant report being attached at the time of assistance.

Where a Police Officer requests access to CCTV images (hereafter referred to as data), either by viewing such data or requesting a copy, then the Police Officer or Force should submit the relevant authorisation documentation in writing for their investigation and request. Unless the Police Force has an Information Data Sharing Agreement that includes the use of CCTV.

When the relevant documentation/form has been completed, the authorised data handler may pass the required data to the Police Officer requiring it. The completed form shall be handed to the Head of Security & Campus Safety or His / Her nominee to be retained for evidential purposes of the release.

SECTION 8 - ACCESS TO RECORDINGS AND DISCLOSURE

Generally, requests by persons outside the University for viewing or copying of or obtaining digital recordings will be assessed on a case by case basis.

Requests from the Police will arise in several ways, including: -

- Requests for a review of recordings, to trace incidents that have been reported.
- Immediate action relating to live incidents e.g. immediate pursuit.
- For major incidents that occur, when images may have been recorded continuously.
- Individual Police Officer seeking to review recorded images within the Control Room.

Requests for access to recorded images from persons other than the Police or the data subject will be considered on a case-by-case basis. The Head of Security & Campus Safety or His / Her nominee will consider such requests to protect the privacy of persons recorded in line with legislative requirements and obligations. Requests for access to data under a Subject Access

request are dealt with by a clear process set out in the operations manual and accompanied by a subject access request form. Members of the public are entitled to apply for a copy of their data under this process. Data will be released only if it is meets the aims and objectives of the System within this Code.

SECTION 8.1 - STANDARDS

It is important that access to, and disclosure of, the images recorded by CCTV is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Users of CCTV will also have to ensure that the reasons for which they may disclose copies of the images are compatible with the reasons or purposes for which they originally obtained those images, following Data Protection legislation. All control room staff are aware of the restrictions set out in this code of practice concerning access to, and disclosure of, recorded images.

- Access to recorded images will be restricted to staff who need to have access to achieve the purposes of using the equipment.
- All-access to the medium on which the images are recorded will be documented

Disclosure of the recorded images to third parties or other individuals or departments within the University will be made only in the following limited and prescribed circumstances:

- Law enforcement agencies where the images recorded would assist in a specific criminal inquiry.
- Prosecution agencies.
- Authorised relevant legal representatives.
- Where it is decided after full consultation by the Head of Security & Campus Safety, University Senior Management, Data Controller and Law Enforcement that the public's assistance is needed to identify a victim, witness or perpetrator about a criminal incident, images from the system will be provided to the media. As part of that decision, the wishes of the victim of an incident will, where possible, be considered.
- People whose images have been recorded and retained and disclosure is required under a Subject Access Request..

All requests for access or disclosure will be recorded. Decisions on access to recorded images by persons other than Police officers will be made by the Head of Security & Campus Safety or His / Her nominee, if required the final decision will be made by the Data Protection Officer. Requests from the Police will not normally be refused but will require a formal request, signed by an officer using the requisite form unless an Information Sharing Agreement including the use of CCTV is in place with the Police Force.

If the Head of Security & Campus Safety or His / Her nominee or Data Protection Officer denies access or disclosure, the reasons will be documented and forwarded to the Control Room Operators for filing.

If access to or disclosure of the images is allowed by the Head of Security & Campus Safety or His / Her nominee in non-Police cases or by a member of the control room staff where the proper format has been followed - as above - in Police cases, then the following will be documented:

- The date and time at which access was allowed or the date on which disclosure was made. *

- The reason for allowing access or disclosure. *
- The extent of the information to which access was allowed or which was disclosed. *
- Routine disclosure to the Police will be documented by control room staff using the appropriate forms, which will be filed with a copy of the authorising officer's written request (see above).
- Requests for non-police disclosures will be forwarded to the Head of Security & Campus Safety.*

*See also below, at 'Access by Data Subjects'.

SECTION 8.2 - ACCESS BY DATA SUBJECTS

All staff involved in monitoring or handling image data will proceed in accordance with the following protocol in respect of Subject Access Requests. Data subjects will be provided with a standard subject access request form which:

- Requires individuals to provide dates and times when they visited University and their location - for example which Area within the University
- The individuals will provide two photographs of themselves - one full-face one side view with the completed form.
- They will provide to the person receiving the application proof of their own identity e.g. a utility bill, a driving licence or a passport.
- They will be asked whether they would be satisfied with merely viewing the images recorded or if they want a copy.
- You can see the University Privacy Statement and Policy at the following link should need more information:
  - Staff Statement: https://www.essex.ac.uk/staff/your-information-your-rights/privacy-notice-staff
  - Students Statement: https://www.essex.ac.uk/student/my-essex/privacy-notice-students
- A written decision on their request will be sent to them within one month of receiving a valid request.

To find out more about Subject Access Requests and the process within the University please visit: https://www1.essex.ac.uk/records_management/request/default.aspx

SECTION 8.3 - RIGHTS OF DATA SUBJECTS

The procedure outlined in the Subject Access Request policy enables the University or their nominee to inform individuals as to whether or not images have been processed by the CCTV system. The University is not obliged to comply with a request under this section unless it is supplied with such information as it may reasonably require to satisfy itself as to the identity of the person making the request and to locate the information which that person seeks in relation to CCTV.

Where the University cannot comply with the request without disclosing information relating to another individual who can be identified from that information, it is not obliged to comply with the request unless:

- The other individual has consented to the disclosure of the information to the person making the request, or

- It is reasonable in all the circumstances to comply with the request without the consent of the other individual.

In the case of a request under Subject Access rules, where the images form part of a criminal investigation and to release them would interfere with that investigation, the University may decline their release.

SECTION 9 – SUPPORT DOCUMENTS

This document is also supported by the following documents.

- Body Camera Policy
- University of Essex Data Protection Policy
- University of Essex Privacy statement

APPENDIX 1: HOW TO APPLY FOR ACCESS TO CCTV EXTERNAL

These notes explain how you can find out what information, if any, is held about you on the CCTV System.

YOUR RIGHTS

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. The University will only give that information if it is satisfied as to your identity. If the release of the information will disclose information relating to another individual(s), who can be identified from that information, the University is not obliged to comply with an access request unless

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

THE UNIVERSITY RIGHTS

The University may deny access to information where the legislation allows. The main exemptions concerning information held on the CCTV System are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders

And giving you the information may be likely to prejudice any of these purposes.

THE APPLICATION FORM:

(N.B. ALL sections of the form must be completed. Failure to do so may delay your application. The information recorded in this form will be securely held and not shared with other parties without your express consent.)

Section 1 - Asks you to give information about yourself that will help the University to confirm your identity. The University has to ensure that the information it holds is secure and it must be satisfied that you are who you say you are.

Section 2 - Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full-face and side view photograph of you.

Section 3 - asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

Section 4 - You must sign the declaration

When you have completed and checked this form, take or send it together with the required TWO identification documents and photographs to Data Protection Officer, University of Essex, Wivenhoe Park, Colchester, Essex, CO4 3SQ. If you have any queries regarding this form or your application, please email secspvrs@essex.ac.uk the University Head of Security & Campus Safety.

Section 1	
Title	
Surname/Family Name	
First Names	
Maiden Name/Former Names	
Sex	
Height	
Date of Birth	
Place of Birth (Town / County)	
Your Current Address (to which we will reply)	
Address 1	
Address 2	
City / County	
Post Code	
Telephone Number	
Section 2	
To help establish your identity your application must be accompanied by TWO official documents that between them clearly show your name, date of birth and current address For example, a birth/adoption certificate, driving licence, medical card, passport or another official document that shows your name and address	
Section 3	
You have the right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to?	
View the information and receive a permanent copy	YES / NO
Only view the information	YES / NO
Section 4	
DECLARATION **(to be signed by the applicant)**	
The information that I have supplied in this application is correct and I am the person to whom it relates	
Signature	
Date	
Warning - a person who impersonates or attempts to impersonate another may be guilty of an offence. NOW – please complete Section 4 and then check the “CHECK” box before returning	

the form. If the information you have requested refers to a specific offence or incident, please complete this section. Please complete a separate box in respect of different categories/incidents/involvement. Continue a separate sheet in the same way, if necessary. If the information you require relates to a vehicle, property, or another type of information, please complete the relevant section overleaf.	
Were you:	
A person reporting an offence or incident	
A witness to an offence or incident	
A victim of an offence	
A person accused or convicted of an offence	
Other – Please explain	
Date(s) and time(s) of incident	
Place Incident Happened	
Brief details of the incident	
Before returning this form please check:	**Have completed ALL sections in this form?**
	Have you enclosed TWO identification documents?
	Have you signed and dated the form?
Further Information:	
The information collected in this form will be used for the purposes of processing your request. It will be held in compliance with the data protection legislation and in accordance with the University of Essex Data Protection Policy. This form will be kept for 3 year and will be held in a secure online folder. Further information and advice may be obtained from:	
Data Protection Officer, The University of Essex,	The Office of the Information Commissioner Wycliffe House

Wivenhoe Park, Colchester, Essex, CO4 3SQ	Water Lan Wilmslow Cheshire SK9 5AF
Telephone:	**Telephone:** 01625 545 745
Please note that this application for access to information must be made direct to University and NOT to the Data Protection Commissioner	
OFFICIAL USE ONLY	
Please complete ALL of this section (refer to CHECK box above)	
Application checked and legible?	
Date Application Received	
Identification documents checked?	
Details of two documents	
Documents returned	
Member of staff name	
Member of staff signature	
Location	
Date	

APPENDIX 2: REQUEST FOR VIEWING/EXTRACT OF FOOTAGE (INTERNAL ONLY)

Send To: **Head of Security & Campus Safety** **University of Essex Colchester Campus** **Estates & Campus Services**	**Name:**	
	Position:	
	Department:	
	Contact No:	
Date of Request:		
Date of Incident:		
Time(s) of Incident:		
Description of Incident (Please include place of incident and give as much details as possible)		
Reason for Request:		
If for Internal Investigation for employees or contractors, the below needs a signature		
HR Manager or Investigator Signature:		
Head of Security & Campus Safety / Nominee Signature:		
Does it fit the Aims & Objectives of the System?	Yes / No	
Your request has been:	Agreed / Denied	
If denied, the reason for denial:		
Please note that CD/DVD's will only be held for a maximum of 31 days from the date of this request.		

APPENDIX 3: DISCLOSURE OF DATA TO PERSONS OTHER THAN THE POLICE

Section A -Description of Data required to be disclosed (To be completed by Head of Security & Campus Safety or his / her nominee or the University Data Protection Officer)

Discs / USB

View:	Take Possession of:	Disc / USB Number	Disc No. (S) and Date

Data Contained Within Documents

View:	Take Possession of:	Original	Copy	Given Verbally

Description of document (s)

Disclosure of Data Contained Within Computerised Records

View	Take Possession of:	Disc / USB	Printout	Given Verbally

(State what data is required and where data stored (i.e. the home address of named person; occupant of named address etc from the system *what data is required and where data stored)*

University Representative Making Disclosure

Department	
Name	
Signature	
Date	

Section C – Reason Data Required *(To Be Completed By Person Requesting Data)*

I can confirm that the above data is required by me for any of the following reasons contained within) the provisions of the General Data Protection Regulation and the Data Protection Act 2018.

For the purpose of safeguarding national security	
The prevention or detection of crime	
For the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings)	
Is otherwise necessary for the purposes of establishing, exercising or defending legal rights	

Name	
Position (If Applicable)	
Business / Agency	
Business / Agency / Home Address	
Signature	
Date	
Reference Number:	

The information collected in this form will be used for the purposes of processing your request. It will be held in compliance with the data protection legislation and in accordance with the University of Essex Data Protection Policy. This Form will be held for 3 years. Further information and advice may be obtained from: https://ico.org.uk/

University Data Protection Officer:

Address: The University of Essex, Wivenhoe Park, Colchester, Essex, CO4 3SQ

Email: dpo@essex.ac.uk