

**Policy & Standards for
CCTV Operation at The University of Essex (Southend Campus)**

Index

1. Introduction
 - 1.1 System Description
 - 1.2 Purpose of the System
 - 1.3 Operating Principles
 - 1.4 To Whom this Document Applies
2. Policy
3. Operating Standards
 - 3.1 Processing CCTV Images
 - 3.2 Quality of Recorded Images
 - 3.3 Appropriate Signage
4. Access to / Disclosure of CCTV Images
 - 4.1 Request from a Data Subject for Access / Disclosure
 - 4.2 Request from a Data Subject to Prevent Processing / Automated Decision Taking
 - 4.3 Request from a Third Party for Access / Disclosure
5. Disclosure to the Police
6. Complaints Procedure
7. Monitoring Compliance with the General Data Protection Regulations (GDPR and the CCTV Code

Annexes:

- A-** Information Leaflet for the Operation of CCTV at Essex University
- B-** GDPR, Subject Access Request Form CCTV at Essex University
- C-** GDPR, Third Party Request Form CCTV at Essex University.

Issued on 1st October 2017

This Policy is the property of The University of Essex and should not be published, distributed or copied without the permission of the Director of the Estates Management Section, The University of Essex, Wivenhoe Park, Colchester, Essex, CO4 3SQ. Tel: 01206 873411. Any suggested alterations, amendments or comments should be discussed with the FM provider Southend Campus Security Manager and then sent to the University Security Manager.

Paul Humphreys, Security Manager

University of Essex, Wivenhoe Park, Colchester, Essex, CO4 3SQ

REVIEW DATE: June 2019 (or on any legislation change or Government guidance)

Policy Statement

The University seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors and contractors, whilst within or situated on University premises. To this end, CCTV cameras and recording devices are deployed within and around the University Estate to assist in the prevention, investigation and detection of crime, the apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings), public, employee and student safety and for monitoring security of premises at The University of Essex Southend Campus.

This Policy document has been implemented to ensure that the deployment and control of CCTV resources is proportionate and lawful under the terms of the General Data Protection Regulations, (GDPR) and the CCTV Codes of Practice. This Policy refers to the Southend Campus. A separate policy is issued for Colchester and Loughton.

Chris

Digitally signed by Chris Oldham

Oldham

Chris Oldham

Sara Stock

Director Estate Management Section

University Records Manager

University of Essex

University of Essex

Paul Humphreys

Ian Bradley

Security Manager

FM Provider Security Manager

University of Essex

Southend Campus

1. Introduction:

This document details the operating policy and standards for the closed, circuit television (CCTV) systems installed at The University of Essex Southend Campus, in accordance with the requirements of GDPR and the Code of Practice (CCTV Code) issued by the Information Commissioner.

The CCTV systems at The University of Essex are registered as part of the University's entry on the Data Protection register which is held by the Information Commissioner.

1.1. System Description:

The CCTV system installed in and around The University of Essex Southend Campus, Gateway, Clifftown Studios and University Square Accommodation Buildings comprises of fixed IPTV cameras. The Forum also has a fixed CCTV Camera system for the building. This is controlled by the Security Company within the Forum Building. These cameras provide fields of view encompassing approaches to buildings, entrances, building property, communal areas (including lifts and foyers) and secure areas. All cameras are linked to a digital hard disk recorders situated in the Gateway Building. This provides data management and recording facilities locally to Security Staff. The Southend Campus Manager, FM provider Security Manager, ISS Data Manager and the Forum Security Manager (Forum cameras only) or their designated representatives are the only authorised Security, ISS, Forum staff who may access images to the system, for the purpose of storing or reviewing footage, on strict permission from the FM provider Security Manager and once the procedures laid down in section 4 of this document have been met.

1.2. Purpose of the System:

The purpose of the CCTV systems in use at the University of Essex Southend Campus is to enable the prevention, investigation and detection of crime and monitoring of the security and safety of people and premises at The University of Essex Southend Campus.

1.3. Operating Principles

To ensure compliance with GDPR, personal data, including images recorded on the CCTV systems, must at all times be processed in line with the following Principles:

- Fairly and lawfully processed;
- Processed for limited purpose and not in any manner incompatible with the purpose of the system;
- Adequate, relevant and not excessive;
- Accurate;

- Not kept for longer than is necessary (31 days on hard drive)
- Processed in accordance with the individuals' rights;
- Secure;

1.4.To Whom this Document Applies:

The University of Essex (the “Data Controller”) and its employees or agents who operate, or supervise the operation of the CCTV systems at The University of Essex Southend Campus; namely Campus Manager, FM Security Management and staff, ISS authorised staff, Forum authorised staff, and the University Records Manager.

2 Policy:

2.1. Scope:

2.1.1. This Policy applies to all parts of the University estate Southend.

2.1.2. This Policy does not apply to the AVMS systems located in lecture theatres and halls for the purpose of recording lectures for distribution to students, or the Students Union who control their own CCTV system within their establishment. The AVMS section and the Students Union are responsible for ensuring they comply with the DPA and the CCTV Codes of practice.

2.2. Personal Data (i.e. images of individuals obtained by the University of Essex CCTV systems) may **only** be used in connection with the purpose set out in section 1.2.

2.3. The ability to view live and historical CCTV data controlled by the University of Essex is only available from the FM Security Manager and to authorised persons only: (see below at 2.5)

2.4. Except where a request has been granted for third party access to certain specified recorded CCTV image (see below at 2.5), CCTV images are not displayed in the presence of any unauthorised person.

2.5. For the purpose of viewing CCTV images, an authorised person is defined as an employee or appointed person acting on behalf of the University of Essex who has an operational responsibility for either, the prevention, investigation and detection of crime and / or the monitoring of the security and safety of students, staff, visitors or contractors or property at the University of Essex Southend.

2.6. No images may be captured from areas in which individuals would have an expectation of privacy (i.e. toilets, changing facilities, study bedrooms in halls of residence etc).

2.7. At all times the operation of the CCTV systems are to be conducted in accordance with the procedures set out in this document.

2.8. The University Security Manager and FM Security Manager are responsible for ensuring that CCTV systems and camera specifications for new installations at the University of Essex Southend Campus comply with the DPA and the CCTV Code.

2.9. Only the advised contractor for the University of Essex Southend Campus may be used to install or maintain the CCTV system on the University estate.

2.10. Changes in the use of the CCTV system may only be implemented in accordance with the DPA and the CCTV Code. The University Records Manager must be consulted before any changes take place.

3. Operating Standards:

3.1. Processing CCTV Images:

It is imperative that access to, and security of the images is managed in accordance with the requirements of the GDPR and the CCTV Code. At all times the following standards are to be applied:

3.1.1. CCTV images are not to be retained for longer than is necessary. Data storage is automatically managed by the CCTV digital recorders, which use software programmed to overwrite historical data in chronological order to enable the recycling of storage capabilities. This process produces an approximate 21 day rotation in data retention.

3.1.2. Provided that there is no legitimate reason for retaining the CCTV images (such as for use in legal proceedings), the images will be erased following the expiration of the retention period.

3.1.3. If CCTV images are retained beyond the retention period, they are to be stored in a secure place to which access is controlled and are to be erased when no longer required.

3.2. Quality of Recorded Images:

Images produced by the recording equipment must be as clear as possible in order that they are effective for the purpose for which they are intended. The standards to be met under the CCTV Code are set out below.

- Recording features such as the location of the camera and / or date and time reference must be accurate and maintained.

- Cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established.
- Consideration must be given to the physical conditions in which the cameras are located i.e. additional lighting or infrared equipment may need to be installed in poorly lit areas.
- Cameras must be properly maintained and serviced to ensure that clear images are recorded and a log of all maintenance activities kept.
- As far as practical, cameras must be protected from vandalism in order to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit with vandal resistant casing.

3.3. Appropriate Signage:

Signs must be placed so that members of the public are aware that they are entering an area which is covered by CCTV. Signs must:

- Be clearly visible and legible
- Be of a size appropriate to the circumstances
- Contain the following information
 - The name of the Data Controller (i.e. The University of Essex)
 - The purpose(s) of the scheme
 - A contact telephone number for enquiries

4. Access to /Disclosure of CCTV Images:

Requests for access to, or disclosure of (i.e. provision of a copy), images recorded on the CCTV systems from third parties (i.e. unauthorised persons) will only be granted if the requestor falls within the following categories

- Data Subjects (i.e. persons whose images have been recorded by the CCTV systems)
- Law enforcement agencies (where images recorded would assist in a specific criminal enquiry)
- Prosecution agencies (including the Security Manager in the course of staff or student disciplinary proceedings)
- Relevant legal representatives of data subjects

The contact point indicated on the CCTV signs around the University of Essex Southend Campus should be available to all staff, students, visitors and contractors. Security Officers who staff the contact point should be familiar with this document

and the procedures to be followed in the event that an access request is received from a Data Subject or a third party.

4.1. Request from a Data Subject for Access / Disclosure:

Data Subjects (i.e. persons whose images have been recorded by the CCTV systems) have various rights under GDPR, including the right to be informed that personal data (i.e. images of themselves) are being recorded and the right to view such images. Should any person visiting the University of Essex Southend Campus have questions concerning the operation of the CCTV systems or their rights with respect to any images of them recorded by the systems, the following procedure must be complied with:

- 4.1.1. The Data Subject should be directed to an authorised person (normally the on duty FM provider Security Manager / Supervisor).
- 4.1.2. The Data Subject is to be provided with a copy of the Information Leaflet attached at Annex A (which describes the purpose and operation of the CCTV systems at the University of Essex Southend Campus).
- 4.1.3. The Data Subject is to be provided with a copy of the Subject Access Request Form attached at Annex B, this will enable them to make a formal request to view/ receive copies of images of themselves.
- 4.1.4. The Data Subject is to send the completed Subject Access Request Form to the FM provider Security Manager together with a £10 search fee.
- 4.1.5. The FM provider Security Manager will liaise with the University Security Manager or Records Manager to:
 - Determine whether the request should be complied with
 - Ensure that the relevant images are located
 - Determine whether third party images (i.e. images of persons other than the Data Subject) are contained within the images
 - Ensure that any third party images are disguised or blurred before access or disclosure is granted
- 4.1.6. The FM provider Security Manager must ensure that a written acknowledgement is sent to the Data Subject as soon as practicable after receipt of the completed Subject Access Request Form. The written acknowledgment is to contain the following:
 - The name of the Data Subject
 - A request for the payment of the £10 search fee (if this has not accompanied the completed form)

- A request for further information to enable identification of the Data Subject or the relevant images (if necessary)
- A confirmation of the start date for the response period (see below);
- The name and signature of the FM provider Security Manager

4.1.7 Subject Access Requests are to be processed as soon as practicable and in any event within 20 days of the letter acknowledging receipt of sufficient information to enable identification of the Data Subject and / or relevant images, and the £10 search fee.

4.1.8 Once the images have been located and the FM provider Security Manager, University Security Manager or University Records Manager have agreed that a Subject Access Request can be complied with, the FM provider Security Manager must provide the Data Subject with written notice containing the following:

- The name of the Data Subject
- The date of receipt of the completed Subject Access Request Form and the £10 search fee
- A description of personal data (i.e. images of the Data Subject recorded on the CCTV systems at the University of Essex between (insert time) on (insert date)
- If the Data Subject elected in their completed Subject Access Request Form to view the images at The University of Essex, an invitation to contact the Security Manager to arrange a viewing of the images during normal working hours
- If the Data Subject elected in their completed Subject Access Request Form to receive a copy of the relevant images, references to a CD-ROM being enclosed which contains the relevant images of the Data Subject and the blurring of any third party images (if applicable)
- The name and signature of the FM provider Security Manager

4.1.9 If the Data Subject elected in their completed Subject Access Form to view the images at the University of Essex, immediately following that viewing an entry needs to be made in the CCTV Operating Log Book recording:

- The name(s) of the Data Subject and all other attendees
- The date and time of the viewing
- The location where the viewing took place

4.1.10. If the FM provider Security Manager, University Security Manager or Records Manager agree that a Subject Access Request cannot be complied

with, the Security Manager must provide the Data Subject with written notice containing the following:

- The name of the Data Subject
- The date of receipt of the completed Subject Access Request Form and the £10 search fee
- The reason for refusing to grant access to / supply the images requested (i.e. compliance with the request would, or would likely to, prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders; the images have already been erased etc)
- The name and signature of the FM provider Security Manager
- A refund of the £10 search fee.

4.2 Requests from a Data Subject to Prevent Processing / Automated Decision Taking:

In addition to rights of access, Data Subjects also have rights under GDPR to prevent processing (i.e. monitoring and recording CCTV images) likely to cause substantial and unwarranted damage to that person, or prevent automated decision taking (i.e. through the use of visual recognition software) in relation to that person. It is unlikely that either ground would apply to the operation of the CCTV systems at The University of Essex. However, should any person visiting The University of Essex have any concerns regarding the operation of the CCTV systems, the following procedure must be complied with:

4.2.1. The Data Subject should be directed to the University Records Manager to determine whether the Data Subject is making a request to prevent processing or automated decision making. If the University Records Manager determines that the Data Subject is instead making a Subject Access Request, the procedure set out in paragraph 4.1 above should be followed.

4.2.2. The University Records Manager will liaise with the Security Manager to determine whether the access / disclosure is necessary for the prevention, investigation and detection of crime, or the apprehension and prosecution of offenders, and whether the request should therefore be complied with.

4.2.3. The Security Manager must ensure that a written acknowledgment is sent to the Data Subject as soon as is practicable and in any event within 20 days of receiving the request containing the following:

- The name of the Data Subject
- Either a confirmation that: the University of Essex will comply with the request to prevent processing of the CCTV images likely to cause substantial and unwarranted damages to the Data Subject; or that;

- The University of Essex will not comply with the request to prevent processing of the CCTV images likely to cause substantial and unwarranted damages to the Data Subject and the reasons for this decision; or that;
- No automated decision in respect of the CCTV images has been made by the University of Essex.

4.3 Requests from a Third Party for Access / Disclosure:

Unlike Data Subjects, third parties who wish to have access to, or a copy of, CCTV images (i.e. images not of the person making the request) do not have a right under GDPR to access, and care must be taken when complying with such requests to ensure that neither the GDPR or the CCTV code are breached. As noted above, requests from third parties will only be granted if the requestor falls within the following categories:

- Law enforcement agencies (where images recorded would assist in a specific criminal enquiry (see para 5 for further details))
- Prosecution agencies (including University Managers in the course of investigating or pursuing Staff or Student disciplinary proceedings)
- Legal representatives of the Data Subject

In order to ensure compliance with the GDPR and the CCTV Code the following procedure must be complied with:

4.3.1. The Third Party should be directed to an authorised person (normally the FM provider Security Manager)

4.3.2. The Third Party must be provided with a copy of the Third Party Request Form attached as Annex C to enable them to make a formal request to view / receive copies of images of themselves. They may complete the form at the time and return it subsequently to the FM provider Security Manager.

4.3.3. Any completed Third Party Request Form must then be given to the FM provider Security Manager to pass on to the University Security Manager or Records Manager.

4.3.4. The FM provider Security Manager will liaise with the University Security Manager or Records Manager to:

- Determine whether the request should be complied with, including whether a request for the provision of the storage media on which images are saved should be complied with.
- Ensure that the relevant images are located

- Determine whether third party images (i.e. images of persons other than the intended Data Subject) are contained within the images
- If applicable, ensure that any third party images are disguised or blurred before access or disclosure is granted

4.3.5. Once the images have been located and the FM provider Security Manager and University Security Manager or Records Manager have agreed that a Third Party Request can be complied with, the FM provider Security Manager must provide the Third Party with written notice containing the following:

- The name of the Third Party
- The date of receipt of the completed Third Party Request Form
- A description of personal data (i.e. images of the Data Subject (s) recorded on the CCTV systems at the University of Essex between (insert time) on (insert date))
- If the Third Party elected in their completed Third Party Request Form to view the images at the University of Essex, an invitation to contact the Security Manager to arrange a viewing of the images during normal working hours.
- If the Third Party elected in their completed Third Party Request Form to receive a copy of the relevant images, references to a CD-ROM being enclosed which contains the relevant images of the Data Subject and the blurring of any third party images (if applicable)
- The name and signature of the FM provider Security Manager.

4.3.6. If the Third Party elected in their completed Third Party Request Form to view the images at the University of Essex, immediately following the viewing an entry must be made in the CCTV Operating Log Book recording:

- The name(s) of the Data Subject and all other attendees
- The date and time of the viewing
- The location where the viewing took place
- Details of the footage viewed including which camera produced the footage, date and time of recording

4.3.7. If the FM provider Security Manager and University Security Manager or Records Manager agree that a Third Party Request cannot be complied with, the FM provider Security Manager must provide the Data Subject with written notice containing the following:

- The name of the Third Party
- The date of receipt of the completed Third Party Request Form

- The reason for refusing to grant access to / supply the images requested (i.e. compliance with the request would, or would be likely to, prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders; the images have already been erased etc)
- The name and signature of the FM provider Security Manager

5. Disclosure to the Police:

5.1. If identified, CCTV footage will be freely shared with the Police to aid them in the pursuit of an investigation into criminal activity against the premises or personnel of the University of Essex. In all cases an entry needs to be made in the CCTV Operating Log Book recording:

- The name of the Police Office receiving the copy of the recording
- Brief details of the images captured by the CCTV to be used in evidence, including which camera produced the footage, date and time of recording
- The crime reference number
- The date and time the images were handed over to the Police
- Details of the format in which the images were handed over

5.2. Where information is requested from the Police in pursuit of an investigation unrelated to criminal activity against the premises or personnel of the University of Essex, the University will only make such disclosures on receipt of a Section 29 Data Request Form signed by a Senior Police Officer (inspector or above) and once satisfied of the following:

- That the purposes are indeed relating to crime
- That failure to release would prejudice the Police investigation

(The University Records Manager will always make the final decision)

In all cases an entry will be made in the CCTV Operating Log Book recording:

- The name of the Police Office receiving the copy of the recording
- Brief details of the images captured by the CCTV to be used in evidence
- The crime reference number
- The date and time the images were handed over to the Police

6. Monitoring Compliance with the GDPR and the CCTV Code

An annual assessment will be undertaken by the University Records Manager and the University Security Manager to evaluate the effectiveness of the CCTV systems at the University of Essex and its compliance with the GDPR and the Code. The results of the report will be assessed against the stated purpose of the scheme. If the scheme is not achieving its purpose, remedial action must be undertaken to modify the systems.

Requests from members of the public for access to such reports will be considered by the University Records Manager on a case-by-case basis under the requirements of the “Freedom of Information Act 2000”.

7. Complaints Procedure

Records of all complaints, and any follow up action, will be maintained by the University Records Manager, in accordance with University records retention schedules.

Annex A to

Policy & Standards for CCTV Operation

At the University of Essex
Southend Campus

**INFORMATION LEAFLET FOR THE OPERATION OF CCTV AT THE
UNIVERSITY OF ESSEX**

This leaflet contains information and advice about the operation and management of the closed circuit television (CCTV) systems at the University of Essex Southend Campus. It also tells you about your rights under the GDPR (DPA). In this leaflet “you” means any student, member of staff or interested member of the public, and “we” means the University of Essex.

Why do we have CCTV at the University of Essex Southend Campus?

The University of Essex campus is open to members of the public as well as students and staff. CCTV helps us ensure that students, staff and members of the public are safe and helps with preventing and detecting crime.

How is it controlled?

The GDPR explains how we must look after personal information, including pictures of people captured on CCTV. The Information Commissioner is the official “watchdog” for data protection matters. He has issued a code of practice that tells organisations how to make sure they use CCTV fairly and within the law.

To make sure that the University of Essex complies with the GDPR and the Information Commissioner’s guidance we have introduced policies and procedures that explain how we use CCTV here. The policy explains who can see CCTV pictures, describes how we safely store of images, and includes guidelines for CCTV operators to ensure people’s privacy is respected at all times. The University’s CCTV system is registered with the Information Commissioner.

How does it operate?

The systems are operated by the University of Essex and monitored 24 hours a day, every day of the year. Images from the cameras are recorded and held for a minimum of 21 days. If there is no legitimate reason to keep the recording (an example of a legitimate reason to retain the recording would be a police request) then we automatically ensure that the images are totally destroyed.

Who uses the images?

Only certain people are allowed to look at the images being recorded by cameras. We only show pictures to other people where the GDPR and the Information Commissioner’s guidance allows us to. The only people who can normally see CCTV pictures are those who

are involved in operating or supervising the CCTV system. We will also show pictures to others when it is necessary for prevention and detection of crime or disciplinary offences.

When other people ask to see CCTV pictures we ask them to make a request in writing, explaining why they need to see the pictures. Normally we will only let pictures be seen by:

- Members of the University's Student Discipline Team
- Law enforcement agencies;
- Prosecution agencies; and
- Relevant legal representatives

Can I see the images?

You have the right to access any personal information which is held about you, and that includes CCTV pictures. If you want to see pictures of you recorded by CCTV at the University of Essex you will need to fill in a Subject Access Request Form, which you can get from the Information Desk on Square 3. You will also need to pay a search fee of £10 which would be refundable if access to the images was denied.

So that we can find the relevant pictures you will need to tell us clearly the date, time, where you think you were recorded. We will also need a description of what you were wearing at the time you were filmed. Remember that pictures are usually destroyed 21 days after they were taken. We will respond within 20 days of receiving your completed form and search fee. We will then either explain how you can see the pictures, or explain why we are refusing to let you see the pictures. You cannot ask to see pictures or recordings of other people.

How do I make a complaint?

If you need more information about any aspects of the CCTV systems or wish to make a complaint, please contact the University using the contact details below.

For further information write to:

The University Records Manager,

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

Annex B to

Policy & Standards for CCTV Operation

At the University of Essex

GDPR – SUBJECT ACCESS REQUEST FORM

CCTV AT THE UNIVERSITY OF ESSEX Southend Campus.

(Please use BLOCK CAPITALS to complete this form)

The General Data Protection Regulations provide Data Subjects (individuals to whom “personal data” relates) with a right to access personal data held about themselves, including images recorded on closed circuit television (CCTV) systems.

To enable the University of Essex to deal promptly with your request for access, please complete the form giving as much information as possible to help us identify your personal data.

Under the terms of the DPA, the University of Essex has 20 days to comply with your request. This time period will ordinarily commence on the date that the completed form, containing sufficient information to enable the University of Essex to locate the relevant images, and £10 search fee are received by the Security Manager.

1. PERSONAL DETAILS OF THE DATA SUBJECT

Title Family name

First Name(s)

Date of Birth __ / __ / ____

Permanent Residential Address

.....

.....

..... Post Code

Daytime Telephone Number

Staff/ Student/ Visitor

(Please circle appropriate description)

2. INFORMATION REQUIRED TO LOCATE IMAGES

In order for the University of Essex to identify the images you require access to, please provide the following information:

The exact date(s) and location(s) of the CCTV camera(s) which captured the footage required and approximate time:

.....
.....

Sufficient personal characteristics to enable identification of the Data Subject (a full description including hair colour, clothing etc) together with a photograph. Please use a separate sheet of paper if necessary.

.....
.....

3. ACCESS TO IMAGES (See Section 4 of the Policy)

Assuming the University of Essex is able to locate the required images, please select (X) which of the following will satisfy your request.

..... I would like to view the relevant images at the University of Essex.

..... I would like to be sent a copy of the relevant images.

4. ACKNOWLEDGMENT

I acknowledge that it may be necessary for the University of Essex to contact me to obtain further information to satisfy my identity or to locate my personal data.

I enclose the required £10 search fee (cheques should be made payable to The University of Essex).

I acknowledge the if The University of Essex is of the opinion that complying with this request would, or would likely to, prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders, The University of Essex has the right under the DPA to decline this request.

Signature Date

Return this form to: The Security Manager, The University of Essex, Gateway Building, Elmer Approach, Southend on Sea, Essex SS1 1LW

Annex C to

Policy & Standards for CCTV Operation

At the University of Essex

GDPR – THIRD PARTY REQUEST FORM

CCTV AT THE UNIVERSITY OF ESSEX

(Please use BLOCK CAPITALS to complete this Form)

The General Data Protection Regulations provide Data Subjects (individuals to whom “personal data” relates) with a right to access personal data held about themselves, including images recorded on closed circuit television (CCTV) systems.

Access to the images recorded by the CCTV cameras is restricted and images can only be disclosed in accordance with the DPA and the code of practice issued by the governmental authority that oversees and enforces the DPA, the Information Commissioner. As a consequence, persons who are not involved in the operation or supervision of the CCTV at the University of Essex will only be granted access to, or disclosure of, the recorded images where such access or disclosure is necessary for the prevention, investigation and detection of crime, or the apprehension and prosecution of offenders.

DETAILS OF THE THIRD PARTY APPLICANT

1. Title Family name

First Name(s)

Incident Number (if applicable)

Organisation Name

Organisation Address

.....

.....

..... Post Code

Daytime Telephone Number

Please select (X) which of the following types of organisation you are applying on behalf of:

..... Law enforcement agency

..... Prosecution agency

..... Legal representative

..... Other (please specify)

2. PERSONAL DETAILS OF THE DATASUBJECT (IF APPLICABLE)

Title Family name

First Name(s)

Date of Birth ___ / ___ / ____ Male / Female

3 INFORMATION REQUIRED TO LOCATE IMAGES

In order for The University of Essex to identify the images you require access to, please provide the following information:

The exact date(s) and location(s) of the CCTV camera(s) which captured the footage required and approximate time:

.....
.....
.....

Sufficient personal characteristics to enable identification of the Data Subject (a full description including hair colour, clothing etc) together with a photograph. Please use a separate sheet of paper if necessary.

.....
.....
.....

4. ACCESS TO IMAGES

Assuming the University of Essex is able to locate the required images, please select (X) which of the following will satisfy your request.

..... I would like to view the relevant images at the University of Essex.

..... I would like to be sent a copy of the relevant images.

5. ACKNOWLEDGEMENT

I acknowledge that it may be necessary for the University of Essex to contact me to obtain further information in order to be satisfied as to my identity or to locate the requested images.

I acknowledge that the University of Essex has the absolute discretion to determine whether a request for access to, or disclosure of, the images recorded on the CCTV systems at the University of Essex is necessary for the prevention, investigation and detection of crime, or the apprehension and prosecution of offenders.

I acknowledge that if the University of Essex is of the opinion that complying with this request would, or would be likely to, prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders, The University of Essex has the right to decline this request.

Signature Date

Return this form to: The Security Manager, The University of Essex, Gateway Building, Elmer Approach, Southend on Sea, Essex SS1 1LW