Group CCTV Policy

Policy Control

Version:	Version: Final Draft
Ownership/Review Group:	UCFB Data Privacy Team
Approval:	UCFB Data Privacy Team / Head of Property & Facilities
Last Review Date:	4th November 2019
Next Mandatory Review Date:	Bi annually, from the date of the last review.
Changes to the Policy:	We reserve the right to update this policy at any time, and we will notify staff, suppliers, and partners by email when we make any substantial updates.

1.0 Introduction

The University Campus of Football Business "UCFB" has in place CCTV surveillance systems across its UK campuses. This policy details the purpose, use and management of the CCTV systems at UCFB and defines the procedures to be followed in order to ensure that UCFB complies with relevant legislation and the current Information Commissioner's Office Code of Practice.

UCFB will have due regard to the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018")) and any subsequent data protection legislation, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. Although not a relevant authority, the University will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein.

2.0 Scope

This policy and the procedures defined within applies to all of the UCFB CCTV systems including body worn cameras, webcams, covert installations and any other system capturing images of identifiable individuals for the purpose of viewing and or recording the activities of such individuals. CCTV images are monitored and recorded in strict accordance with this policy.

This policy DOES NOT apply to any Webcam systems located in meeting rooms, lecture theatres or other teaching facilities operated by university, which are used for the purposes of teaching, and to assist with the use of the audio-visual equipment.

This policy applies to all UCFB staff, including contractors, agency staff and temps who operate, or supervise the operation of the CCTV systems, or any individual who has reason to view any images captured by the CCTV systems.

3.0 Summary Overview of the CCTV System

The CCTV systems are owned by UCFB (Floor 14, Piccadilly 111, Manchester, M1 2HY), and managed by the UCFB and its appointed agents. Under the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018")) UCFB is the 'data controller' for the images produced by the CCTV system. UCFB are registered with the Information Commissioner's Office and the registration number is Z3361716.

The Head of Property & Facilities is responsible for the overall management and operation of the CCTV systems, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

The CCTV system operates across the UCFB academic and administrative sites.

Signs are placed at all entrances in order to inform staff, students and visitors that CCTV is in operation. The signage indicates that the system is managed by UCFB.

The Head of Property & Facilities is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.

Cameras are sited to ensure that they cover UCFB premises as far as is possible.

The CCTV system is operational and is capable of recording and storing images 24 hours a day, every day of the year.

Any proposed new CCTV installation across the UCFB estate will be subject to an individual Privacy Impact Assessment which must be reviewed and approved by the UCFB Data Privacy Team prior to installations and/or operation.

4.0 Purpose of the CCTV System(s)

The principal purposes of the UCFB CCTV system are as follows: -

- promote a safe UCFB community and to monitor the safety and security of its premises;
- for the prevention, detection and investigation of crime and other incidents;
- to ensure the safety of staff, students and visitors;
- to assist in the investigation of suspected breaches of UCFB regulations by staff or students.

UCFB seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy.

5.0 Monitoring and Recording

Cameras and the images they capture are not actively monitored in real time.

Images are recorded centrally on servers located securely in the UCFB Data Centre.

In the event of a subject access request, or any other request to view captured and stored images the producer for validation and approval of such request must be followed. See section '8.0 Application for Disclosure of Images' for this procedure and approval process.

The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed and all cameras are checked regularly to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

All images recorded by the CCTV System remain the property and copyright of UCFB.

The monitoring of staff activities will be carried out only under the instruction and supervision of the Head of HR. See section '8.0 Application for Disclosure of Images' for this procedure and approval process.

6.0 Retention & Disposal

CCTV images are not to be retained for longer than necessary, taking into account the purposes for which they are being processed. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce an approximate 28-day rotation in data retention.

CCTV images will only be retained for a period in excess of 28 days for the purpose of providing evidence as part of any on-going staff or student complaint. This CCTV policy should therefore be considered alongside the current student complaints procedure and Staff Handbook / Staff complaints procedure, with specific regard to the retention of images. In consideration of the current student complaints procedure, given the stated timescales to raise and review a complaint, it is not anticipated that images relating any complaints raised will be retained for periods of more than 40 days. However, if complaints are to be raised with the Independent Adjudicator, images may be retained for a period as necessary for the Independent Adjudicator to complete their investigation.

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

All retained CCTV images will be stored securely.

7.0 Compliance with Data Protection Legislation

In its administration of its CCTV system, UCFB complies with the General Data Protection Regulation. Due regard will be given to the data protection principles contained within Article 5 of the GDPR which provide that personal data shall be: -

a) processed lawfully, fairly and in a transparent manner;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed;

and

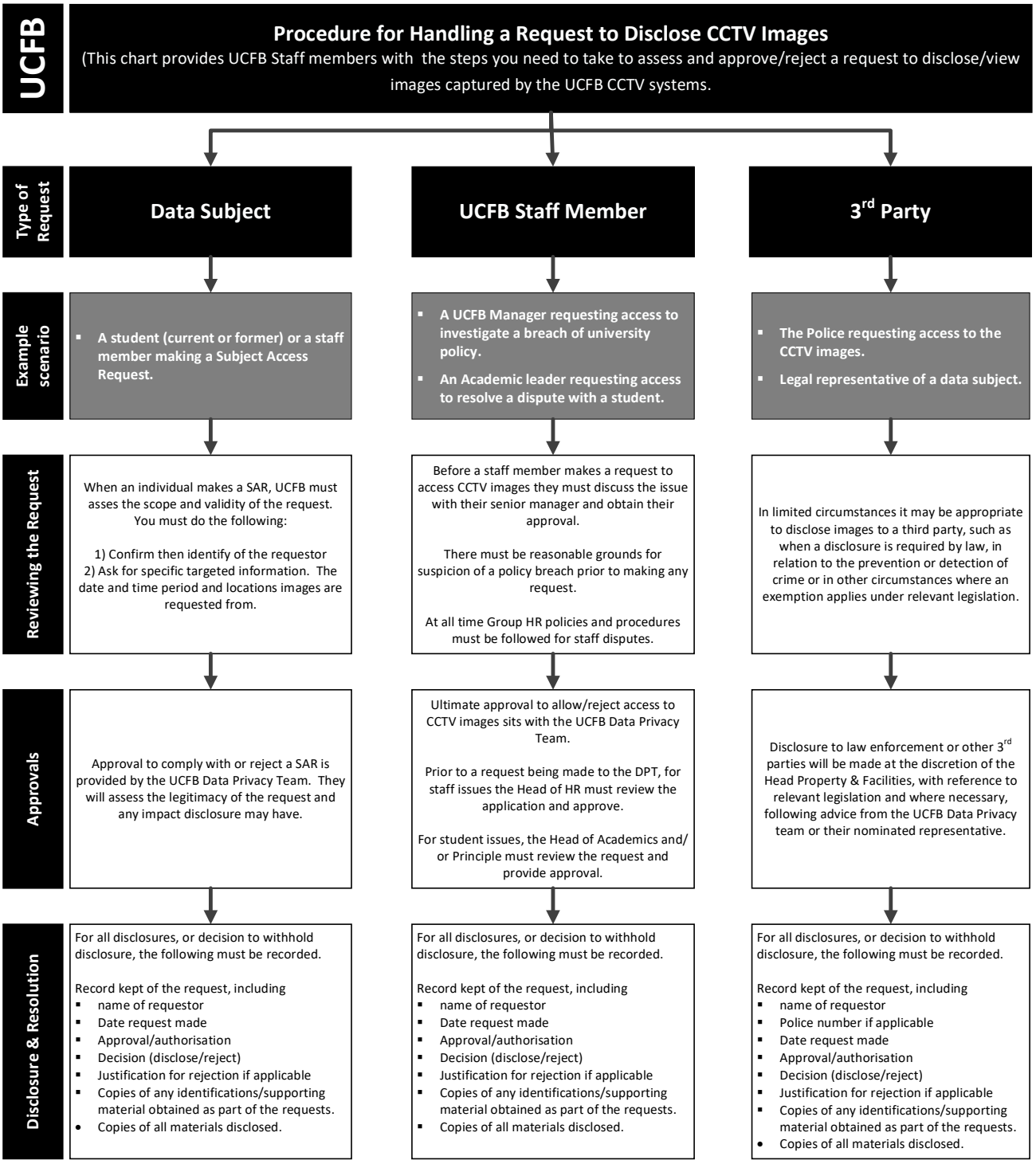
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

It is the responsibilities of the UCFB Data Privacy Team (DPT) to review and approve/reject the installation and operations of CCTV systems across the UCFB estate. These requests will be made to the DPT via a completed Privacy Impact Assessment.

The DPT will also seek assurance from the Head of Property & Facilities that CCTV systems continue to be operated and maintained in line with relevant regulations. In order to do this the DPT will request a completed CCTV checklist for each system at an agreed interval. (see Appendix A for the CCTV checklist.)

8.0 Application for Disclosure of Images.

The following procedure summarised the steps to follow and approvals required when receiving and responding to a request for access to UCFB CCTV images. If you are in any doubt as to the correct procedure to follow, speak to the Head of Property & Facilities or a member of the UCFB Data Privacy Team who will assist.



9.0 Monitoring Compliance

All staff involved in the operation of the UCFB CCTV Systems will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.

All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake data protection training.

Appendix A- Checklist for users of limited CCTV systems monitoring small retail / business premises.

This CCTV system and the images produced by it are controlled by …….. who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998.1

We (……) have considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of customers. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

Item	Checked By	Date	Date of Next Review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.			
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained long enough for any incident to come to light (eg for			

a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Please keep this checklist in a safe place until the date of the next review.

Appendix B - The guiding principles of the Surveillance Camera Code of Practice

System operators should adopt the following 12 guiding principles:

1) Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2) The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3) There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4) There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5) Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6) No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7) Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8) Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9) Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10) There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11) When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12) Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.