University of Chichester CCTV

Policy & Procedures

1. **Introduction**

   This policy sets out the accepted use and management of CCTV equipment and images to ensure the University of Chichester complies with the Data Protection Act 1998, Human Rights Act 1998 and other legislation. Where in this policy there is reference to the Data Protection Act or other legislation this includes all statutory amendments and subordinate legislation and regulations. The University has produced this policy in line with the Information Commissioner's CCTV Code of Practice (www.ico.org.uk).

2. **Why a surveillance camera system is used**

   The University uses closed circuit television (CCTV) images to support the provision of a safe and secure environment for students, staff and visitors and to protect University property. Specifically, the University has installed CCTV systems to:

   - Deter crime
   - Assist in prevention and detection of crime
   - Assist with the identification, apprehension and prosecution of offenders
   - Monitor security of University buildings and areas
   - Assist in traffic management and parking enforcement
   - Promote a safe community environment
   - Assist with the identification of actions that may result in;
     - disciplinary proceedings against staff and students
     - action against contractors providing services to the University

   It is important to recognise that the University respects the privacy and dignity of its staff, students, visitors, contractors and the general public. Therefore:

   - The number of cameras installed on University premises is suitably modest. Locations have been prioritised in order to prevent excessive coverage.
   - The University has positioned cameras so that they only cover pubic or shared areas. No cameras focus directly into private residential areas or offices - although it should be noted that the external parts of such buildings can sometimes be included in the cameras wider field of vision.
   - Camera operators who monitor cameras for the purpose of public space surveillance will receive SIA (Security Industry Authority) Licensing.
   - The position of cameras will ensure that viewing does not intrude into neighbouring domestic areas that border the University's property as far as is practicable.
   - No camera will be hidden or obscured and as far as possible cameras will be placed out of risk of criminal damage.
   - Images will only be examined where there is justification i.e. when investigating an incident, seeking clarification of an event, improving understanding in relation to health and safety or performance matters or when a crime has occurred or is suspected. This has been communicated to everyone involved in the operation of the system

3. Control and administration

In the context of the ICO Code of Practice, the University is the Data Controller. Responsibility for the surveillance system and management thereof rests with the Director (or Acting Director) of Estates Management. Day to day responsibility is delegated to the Facilities Manager (Soft FM) as part of the University's wider security service.

Access to the system is restricted to the following nominated officers:
Director of Estates Management
Acting Director of Estates Management
Facilities Manager (Soft FM)
Facilities Manager (Hard FM)
Residential Services Manager
Duty Managers
IT Technical Lead

The above personnel receive training in the operation of the system and their responsibilities.
If there is a need to review footage, the above personnel can do so using a dedicated and secure PC located in the Duty Manager's office. This location has been chosen to ensure privacy and control. The office is locked at all times when not in use.

4. Storing and viewing surveillance system information

The University's system uses high quality digital cameras to record live images. This data is saved on the system's hard drive then deleted and automatically overwritten after 31 days.

The system allows high-resolution copies of recordings to be made thereby satisfying the requirements of third party requests and law enforcement agencies. In these circumstances, the following procedure and controls are followed:

At the request of the Police, other agency or a third party, a nominated officer may review the recorded footage from the CCTV system to establish whether an incident was captured by any of the cameras.

The nominated officer may then advise the third party making the enquiry whether the incident has been captured and recorded on the system. They will not indicate at this stage to the third party the specific nature of what has been recorded.

Should the Police, an agency or a third party wish to view footage relating to an incident they must complete an Image Removal Form (see Appendix B). This will require the approval of one off the nominated officers. The same procedure applies for requests of duplicate copies.

Images retained for evidential purposes will be retained in a locked area accessible by the system administrator only. Where images are retained, the sys-tem administrator will ensure the reason for its retention is recorded, where it is kept, any use made of the images and finally when it is destroyed. Our images are held for no longer than 31 days, with the exception of evidence for criminal proceedings, student welfare and gross misconduct.

Nominated officers have been informed of the procedures to follow in relation to law enforcement and third party requests. Critically they know not to deviate from this policy and disclose information to others.

Once information has been disclosed to the Police they become the Data Controller.

All requests for access are recorded. If access if denied, the reason is documented.

5. Staying in control

Duty Managers will report any faults or defects in the system as part of their routine work.
An annual maintenance agreement is in place with a suitable contractor to ensure the system in good working order and repaired promptly.
The Facilities Manager (Soft FM) will ensure compliance with the University's policy and procedures through six monthly checks. This involves a review of the system to ensure it is operating correctly and any documentation associated with image removal requests.
An annual review of the University's wider security requirements is conducted to determine whether use of the surveillance system continues to be justified.

6. Letting people know

The University will clearly display signs so staff, students and visitors are aware they are entering an area covered by CCTV. Signs will be displayed on the main access routes into each area covered by the system. Signs will state:

- The University is responsible for the CCTV system in that area
- The purpose(s) of the CCTV System
- Who to contact regarding the operation of the CCTV system

Security staff using mobile surveillance cameras will inform those persons being recorded that the cameras are in use.

This policy will be reviewed annually. Next date October 2018.

Appendix A: Locations of CCTV coverage

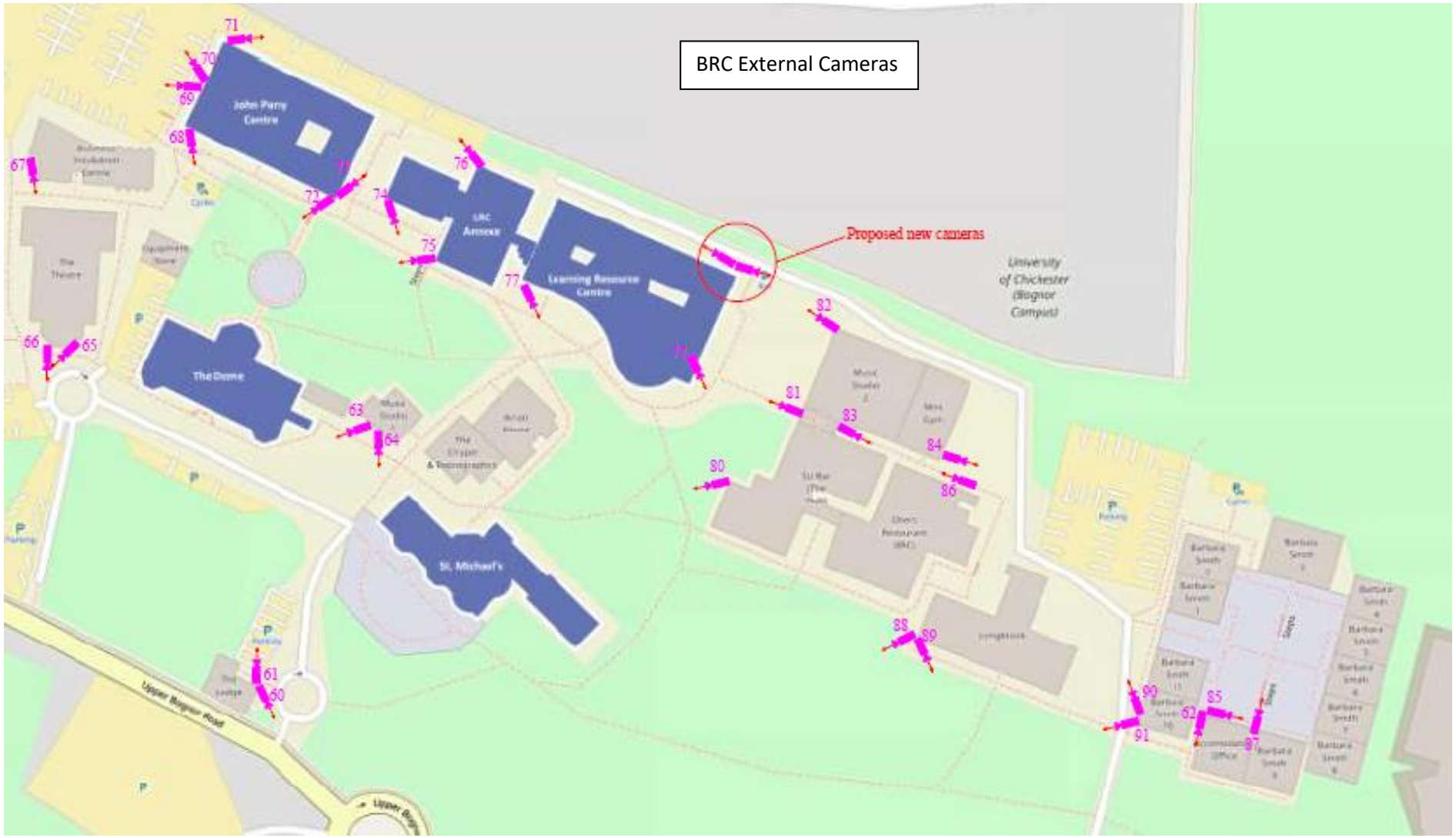
BOC Internal Cameras	DVR			
Building	**Make**	**Model**	**No of Channels**	**Channels used**
Oakland's	VISTA	QP08-1000HF	8	5
LRC – DVR 1	VISTA	QP16-2000HF	16	9
LRC – DVR 2	VISTA	QP16-2000HF	16	10
Havenstoke	VISTA	QP16-2000HF	16	10
Mitre Lecture Theatre	VISTA	QP04-1000HF	4	2
Pinewood	VISTA	QP04-1000HF	4	4
Showroom	ALIEN	618	4	4
Cycle Shed	XENO	XDR404-500	4	4
SARC Phase 2	VISTA	QP08-1000HF	8	4
Springfield 1	VISTA	QP04-1000HF	8	1
Springfield 2 – 4	VISTA	QP04-1000HF	4	3
Springfield 5	VISTA	QP04-1000HF	4	2
Springfield 6	VISTA	QP04-1000HF	4	1
Hammond 1 – 2	VISTA	QP04-1000HF	4	2
Harting Hall	VISTA	QP04-1000HF	4	1
Amberley Hall	VISTA	QP04-1000HF	4	1
Chilgrove Hall	VISTA	QP04-1000HF	4	1
Loxwood Hall 1 & 3	VISTA	QP04-1000HF	4	2
Loxwood Hall 2 & 4	VISTA	QP04-1000HF	4	2
Ifold Hall	VISTA	QP04-1000HF	4	1
Petworth Hall	VISTA	QP04-1000HF	4	1
Midhurst Hall	VISTA	QP04-1000HF	5	1
Fishbourne Hall	VISTA	QP04-1000HF	6	1

Duncton Hall	VISTA	QP04-1000HF	7	1
Ashling Hall	VISTA	QP04-1000HF	8	2
Music & Print	VISTA	QP16-2000HF	16	12

BRC Internal Cameras	**DVR**			
Building	**Make**	**Model**	**No of Channels**	**Channels used**
LRC – DVR 1	VISTA	QP16-2000HF	16	11
LRC – DVR 2	VISTA	QP16-2000HF	16	13
The Dome	VISTA	QP16-2000HF	16	10
Mordington	VISTA	QP08-1000HF	8	4
BMITS	VISTA	QP08-1000HF	8	3
St Michaels	VISTA	QP08-1000HF	8	7
Mordington Cottage	VISTA	QP08-1000HF	8	2
71 Upper Bognor Road	VISTA	QP16-2000HF	16	5
BIC	VISTA	QP08-1000HF	8	4
John Parry	VISTA	QP16-2000HF	16	14
Pavilion Bungalow	VISTA	QP04-1000HF	4	1
Longbrook	VISTA	QP04-1000HF	4	1
Charlotte House	VISTA	QP04-1000HF	4	1
BSH 1	VISTA	QP04-1000HF	4	1
BSH 2	VISTA	QP04-1000HF	4	1
BSH 3	VISTA	QP04-1000HF	4	1
BSH 4-8	VISTA	QP04-1000HF	4	5
BSH 9	VISTA	QP04-1000HF	4	1
BSH 10	VISTA	QP04-1000HF	4	1
BSH 11	VISTA	QP04-1000HF	4	1


BOC External Cameras
Learning Resource Centre
Academic Building
Courtyard
University House
G & H Corridors
Old Chapel
Gym 1 & 2
New Hall
artOne
Facial Recognition
Facial Recognition
Facial Recognition
Proposed Work -
Existing cameras to be relocated to music building. 2 x new dome cameras to be fitted in place.
Proposed Work -
Existing cameras from the laundry building to be relocated to music building
College Lane
Cloisters


BOC External Cameras
53
54
57
56
55
Facial Recognition


BRC External Cameras
Proposed new cameras
John Parry Centre
LRC Annexe
Learning Resource Centre
The Dome
St. Michael's
University of Chichester (Bognor Campus)
Upper Bognor Road
71
70
69
68
67
72
73
74
75
76
77
66
65
63
64
82
81
83
84
86
80
88
89
61
60
90
91
62
85
87

Appendix B: CCTV Data Form

CCTV Data footage supply form

To supply the footage requested for, please accept the following requirements:-

- Provide a date when the CCTV footage will be provided.
- If the request is for the footage to be viewed, to establish possible evidence, ensure as much detail is gathered prior to operating the CCTV. This will cut down the time spent reviewing the CCTV. Areas of interest should be:-
  - Object, type, colour, size
  - The aggrieved persons details (if they were in the area (a good point to start/finish a search from)) ethnicity, build, type/colour of clothing. Time they were in the area
  - Date
  - Time
  - Location
- When providing CCTV footage, ensure:
  - Footage is burnt to CD-R
  - Duplicate the Data for our records
- Provide the Data disk to the head of planning
  - Ensure the data is signed for in the CCTV request folder.
- only ask for personal data which is reasonable and proportionate to the purpose
- All requests made under section 28 of the Data Protection Act are to be referred to the University's Facilities Manager Soft FM or Nominee
- If the request is received outside of standard working hours then staff should contact the University's Duty Manager

CCTV Data Disk

Section 0ne

Circle below

Date Data was recorded	Operators Name	Number of Disks Used	1,2,3,4,5,6,7,8,9,10
		Disk No,	
		Duplicate Disk No,	

Section two

Crime Ref, No.		University Ref, No.	
Date reported to police		Date Reported to UoC	

Section three

Brief description			
Date of Incident		Location	
Time From:			
Time To:		Cam No's	

Section four

Operators Input

The below signatory is signing for the above CCTV data that has been burnt to disk to aid the possible investigation into the alleged incident, detailed in the relating Crime report

Section five

Facilities Manager Soft FM or Nominee		Name:	
Signature of Facilities Manager Soft FM or Nominee			
Date:		Time:	