CANTERBURY CHRIST CHURCH UNIVERSITY

Code of Practice on the Administration of the Control Room

Entry to the Control Room

1 Access to, and disclosure of, the images recorded by CCTV is to be restricted and carefully controlled to ensure the rights of individuals are preserved and ensuring that the data is securely maintained.

2 Images captured by the system will be monitored in the Control Rooms at the relevant sites. The Control Rooms should be secure rooms where the monitors cannot be seen from outside those rooms.

3 There is to be no unauthorised access to the Control Room. Normal access is limited to authorised staff and senior managers. Police officers may enter with the explicit consent of the Operational Manager. The Operational Manager will compile and maintain a record of staff authorised for routine access to the Control Room, including senior managers, which is to be kept in the Control Room for use by Control Room staff.

4 Individuals other than those with routine access may be authorised by the Operational Manager to enter the Control Room for specific purposes. Normally, the Operational Manager provides written authorisation. Each visit will require authorisation and be supervised, at all times, by the Operational Manager or nominee. Such visitors will not be given access to any data that falls within the scope of the Data Protection Act.

5 Where it is not reasonably practicable to secure prior authorisation by the Operational Manager, the most senior member of staff on duty may grant access to persons with a legitimate reason to enter the Control Room.

6 Before granting access to the Control Room, the Operational Manager or the person authorising access must be satisfied as to the identity of any visitor and that the visitor has the appropriate authorisation for entry.

7 All visitors will be required to complete and sign the visitors' log, which includes details of their name, their department or the organisation they represent, the person authorising the visit and the times of entry to and exit from the Control Room. Records will be kept for a period of six years.

8 A record shall be kept of the members of staff on duty in the Control Room at any given time. The records will be kept for a period of one year.

9 Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

Control Room Administration and Procedures

10 An incident log will be maintained in the Control Rooms and details of incidents will be noted together with any consequential action taken.

11 The images obtained comprise personal data and are subject to the General Data Protection Regulation (GDPR) Data Protection Act (DPA) 2018 . All copies will be handled in accordance with the procedures outlined in Code of Practice on the Handling of CCTV Images. The Operational Manager will be responsible for the development of, and compliance with, the working procedures in the Control Room.

12 Recorded images will be reviewed only with the authority of the Operational Manager. Copies of tapes or digital images will only be made for the purposes of detecting crime, in relation to matters affecting safety, evidence for prosecutions, car park management, insurance or where required by law.

13 Any transfer of CCTV images outside the CCTV Control Rooms or the CCTV Surveillance System should be performed using secure and encrypted devices in order to ensure the security and confidentiality of CCTV Images at all times.

14 There must always be at least one Control Room operator present within the Control Room or the Control Room must be kept secured.

Staff Training and Briefing

15 All staff involved in the operation of the CCTV system will be made aware of the purposes for which the scheme was established and the sensitivity of handling CCTV images and recordings, by means of training and access to the University Policy and Codes of Practice.

16 The Operational Manager will ensure all staff, including relief staff, are fully briefed and trained in respect of the necessary functions, operational and administrative, arising within the CCTV control operation.

17 Training in the requirements of the Data Protection Act 1998 and the Codes of Practice will also be provided.

Recording

18 The Control Room system is supported by recording facilities.

19 Where the images are recorded on tape, each tape will be uniquely identified and all activities relating to each tape, for instance date and hours of recording, viewing for specific purpose, copies taken, tapes retained for evidence.

20 When using takes it is important to ensure the quality of images. To this end, it is important that:

- good quality tapes should be used;
- tapes will be erased before being re-used so images are not recorded on top of images recorded previously;
- tapes will not be used when it has become apparent the quality of images has deteriorated.
- if the system records date/time reference, these should be accurate, with a written procedure for ensuring the accuracy of the data.

21 Once a tape has reached its maximum use, its contents will be erased prior to disposal following the University Procedures for confidential waste.

22 Where the images are recorded digitally, the process of identifying retrieval dates and times will be computerised.

22 A tape required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence tape store. If a tape is not copied for the police before it is sealed, a copy may be made later providing it is resealed, witnessed, signed, dated and returned to the evidence tape store.

Request to prevent processing

23 An individual has the right to request the prevention of processing where this is likely to cause substantial and unwarranted damage to that individual.

24 All such requests should be addressed in the first instance to the Operational Manager or the Data Protection Officer, who will provide a written response within one month of receiving the request setting out their decision on the request. A copy of the request and response will be retained for six years.

Retention Periods

25 Unless required for evidential purposes or the investigation of crime, recorded images will be retained on University live systems for no longer than one month from the date of recording.

26 The University recognises that, in accordance with the requirements of the Data Protection Act, 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 there has been no incident that gives rise to the need to retain the recorded images.

27 Erased digital images will be then backed up and permanently erased after a set period, which will be no longer than one month.

28 In the event of the tape or digitally recorded image being required for evidence or the investigation of crime, it will be retained until it is no longer required for evidential purposes or any investigation into a crime has been completed.

Monitoring Procedures

29 The control of the system will remain with the University but at the University's discretion the cameras may be operated in accordance with requests made by the Police during an incident to:

- Monitor potential public disorder or other major security situations;
- Assist in the detection of crime;
- Facilitate the apprehension and prosecution of offenders in relation to crime and public order.

30 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 Operational Manager.

Access to Recordings

31 Access to recorded images will be restricted to staff who need to have access to achieve the purposes of using the equipment.

32 Control Room staff should be aware of the restrictions in relation to access to, and disclosure of, recorded images. Reference should be made to the Code of Practice on Handling Requests from Outside the University for CCTV Images

33 An entry will be logged of any dates the tape/disk/photograph/print was removed from the control room, together with the identity of the person removing it and the reason for such removal.

Photographs

34 Photographs taken from recordings are subject to the same principles and controls of data protection as other data collected in the Control Room. They may only be obtained to assist the identification, apprehension and prosecution of alleged offenders, during staff training and other purposes consistent with the purposes of the CCTV system. Only Control Room staff using equipment in the Control Room may produce photographic material.

35 Photographs will normally be supplied to the police upon reasonable request. The Operational Manager, in consultation with the Data Protection Officer, will consider any requests for viewing photographs other than a Police request.

36 All photographs produced must be recorded along with the identity of the requesting person, date and other appropriate information in the log.

Disposal

37 Video and disc recordings will be destroyed and disposed of following the University Procedures for confidential waste when they are no longer required as evidence. Recordings on any hard disc will be deleted when relevant copies have been made.

38 Photographs will be retained until they are no longer useful as evidence or have become outdated. Thereafter they will be disposed of as confidential waste.

39 At the end of their useful life, all tapes will have their images erased and disposed of as confidential waste.

40 All records will be disposed of as confidential waste at the end of the retention period.

Approval and Review

41 The Senior Management Team approved this Code of Practice in 2006. The Code was reviewed and updated in July 2019 to take account of changes in data protection legislation.

42 The Data Protection Officer will monitor the Code of Practice to ensure compliance with legal obligations and the provisions of the code of practice issued by the Information Commissioner.

Third Party Access Request Form

This form is used to record third party access to CCTV footage or other data.

A1 Details of the CCTV Images to which access is required					
Access required:	CCTV: ☐		BWC ☐	CCTV and BWC☐	
Camera location and time of recording:					
CCTV Image Unique Reference Number:					
Business Reason for access:					
Individual should not be notified:	☐		Date when they can be notified:		

B Details of Person making the Request	
Name and position of the person requiring access:	
Name of employer if different from CCCU:	
Contact details:	
School or Department:	
Request approved by the DPO:	☐ Yes ☐ No
Details of what is Requested:	
CCTV Images to be received in date:	
After use CCTV Images will be:	☐ Retained ☐ Destroyed ☐ Transferred

A2 Details of Additional individuals requiring Access				
Name of individual who needs access to CCTV Images:				
Name of employer if different from CCCU:				
Contact details:				
School or Department:				
Reason for access				
Security:				
Period of access	Start		End	
After use CCTV Images will be:	☐ Retained ☐ Destroyed ☐ Transferred			

C Details of the Security Manager			
I authorise the person named in Section B to access the System under responsibility of the person named in Section A1 for the reason and period specified. Where access is approved, I confirm that this is necessary in accordance with Canterbury Christ Church University Policy.			
Name:		Position:	
Signed:		Date:	

D Details of the Data Protection Officer Approval or Governance Approver			
I authorise the third party access request as detailed in sections A1, B and approved in section C for the duration stated.			
Signed:		Name:	
		Date:	

Third Party Access Request Form

Conditions governing access to CCTV Images

1. Ordinary access to Control Rooms should be strictly limited to the Duty Controllers, authorised Security staff and the Director of Estates and Facilities.
1. Any access by Third Party to the Control Rooms or to CCTV Images should be authorised and recorded. A third party requiring access should communicate in details the reason for accessing the CCTV Images unless an exemption of the Data Protection Act 2018 would apply. If this is the case, the University DPO should be consulted before disclosure.
2. Whenever this would be required, a third party requesting access to CCTV Images should sign a confidentiality agreement.
3. Any CCTV images transferred or retained outside the CCTV Control Rooms or the CCTV Surveillance System should be given a unique reference number. Transfer of CCTV Images should be recorded in a register managed by Security.
4. Any transfer of CCTV images outside the CCTV Control Rooms or the CCTV Surveillance System should be performed using secure and encrypted devices in order to ensure the security and confidentiality of CCTV Images at all times.

For the purposes of this form, a Third Party might be:

1. A member of University staff who does not have access to CCTV images as part of their daily job but might require access for a legitimate business purposes.
2. An employee of an external organisation (i.e. a contractor) who needs access in order to perform activities on behalf of the University.
3. A Police Officer or any other Officer requiring access for the performance of their public duty
4. Any other individuals requesting access to CCTV Images

Further information regarding access to CCTV Images by a Third Party

1. In order to facilitate access to CCTV by a Third Party, an official request is to be completed and submitted to the DPO for approval before access is granted.
2. On a case-by-case basis, Police Officers or other Public Officers may be granted access to CCTV images with the explicit consent of the Security Manager only. Access will be then notified to the University Data Protection Officer at the earliest convenience.
3. Any persons authorised to enter the Control Room or CCTV Images should be supervised at all times.
4. Access to CCTV Images should be granted on a need to know basis. This means only when and if necessary for the specific reason for which access was granted. Unnecessary Third Party access to CCTV Images should be considered a breach of confidentiality and reported to the University DPO.
5. Anyone who is granted operational access to CCTV Images should treat all material as confidential, and not to act upon it, or disclose it to any other person except as specified on the access request. The confidentiality of any private or personal data that they may view inadvertently during the course of access should be preserved as any failure to do so would constitute a breach of confidentiality and may be subject to formal investigation.
6. Unauthorised access and disclosure of Personal Data may constitute a criminal offence and may be subject to formal investigation.
7. On signing the Third Party Access Request Form, both the person who is to be provided with the access to another users' data and those providing the authority are certifying that they have read, understood and agree to these requirements.

Completed form to be sent to information.governance@canterbury.ac.uk on completion for filing