UNIVERSITY OF EAST ANGLIA

SURVEILLANCE CAMERA SYSTEM CODE OF PRACTICE

Report Control Information

Title:	CCTV Code of Practice
Date:	01 January 2020
Version:	2
Authors:	Security Services
Quality Assurance:	Executive Team and Data Protection Officer
Security Class	Open

Revision	Date	Revision Description
v.1		Approved by Aaron Grant
v.2	01/01/19	Updated to reflect changes to law (GDPR, DPA2018) and surveillance tools and coverage

1 Introduction

1.1 The University of East Anglia operates a comprehensive surveillance system (referred to in this document as 'the System'), incorporating fixed Closed Circuit Television System (CCTV) cameras, mobile dashboard cameras (dash cams), Body Worn Video (BWV) worn by UEA security staff, and Automatic Number Plate Recognition (ANPR) technology.

1.2 Cameras are located throughout the main campus and the University Village and are monitored from a secure central room on the main campus (the Control Room).

1.3 The University has produced this policy in line with the Information Commissioner's CCTV Code of Practice[1], and, where relevant, the Surveillance Camera Commissioner's Code of Practice[2].

1.4 The System is owned by the University of East Anglia and the Control Room is staffed by personnel directly employed by the University.

1.5 This code of practice has been prepared for the guidance of Managers and the Operators of the System, and has been reviewed by Norfolk Constabulary

1.6 This code of practice is also designed to satisfy the University community that is students, staff and visitors that the use of surveillance cameras within the University is subject to the correct supervision and scrutiny. It is of

[1] https://ico.org.uk/for-organisations/guide-to-data-protection-1998/encryption/scenarios/cctv/
[2] https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

fundamental importance that public confidence is maintained by fully respecting individual privacy.

1.7 The underlying purpose of this Code is to ensure the System is used to create a safer environment for staff, students and visitors to the University, and that use of the System is consistent with the obligations imposed on the University by the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA2018), and the Protection of Freedoms Act 2012 (POFA).

1.8 The code is available from the UEA Security Control Room and UEA Estates and Buildings Division Reception. It is also published in the University web pages.

2 Complaints

2.1 The Director of Estates and Buildings and the Head of Transport and Security are responsible for the operation of the System and, in the first instance, ensuring compliance with this Code of Practice. Breaches of the code, or any other misuse of the System, by Control Room staff or other University employees will constitute matters of discipline under relevant conditions of employment.

2.2 Any concerns in respect of the System's use or regarding compliance with this code should, in the first instance, be addressed to the Head of Transport and Security. Any concerns about the use of personal data should be raised with the University's Data Protection Officer, who can be contacted on ex 2431 or via email at dataprotection@uea.ac.uk

2.3 Nothing in this code alters the existing rights of members of the University under relevant grievance or discipline procedures.

3 Statement of Purpose

3.1 The purpose of the System (CCTV, BWV and dash cam) is:

3.1.1 To reduce the fear of crime.

3.1.2 To deter and prevent crime.

3.1.3 To assist with the maintenance of public order by reducing nuisance and vandalism.

3.1.4 To facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order.

3.1.5 To facilitate the control of traffic flow and car parking.

3.1.6 To assist with cases of damage to property or injury to person.

3.1.7 To response appropriately to insurance claims and questions of liability.

3.2 The overall aim is to enhance a sense of safety within the university community.

3.3 System recordings will not be used for anything other than the stated purposes. In particular, the System is not intended to be used for general monitoring of UEA employees, however can be used in a lawful investigation.

3.4 The ANPR System will record the number plates of vehicles entering and exiting the car parks on Campus and will

3.4.1 Support the use of the permit scheme.

3.4.2 Count vehicle use of the site.

3.4.3 Collect data for understanding trends, including understanding times of maximum and minimum use

3.4.4 Collate data collected to contribute to planning future provision of facilities.

4 The System

4.1 The System encompasses the main campus and University Village.

4.2 A map of the campus and its boundaries can be found on the Universities portal https://portal.uea.ac.uk/estates/help.centre/maps.

4.3 The System is in operation for 24 hours a day throughout the whole year.

4.4 All Security staff will have taken the mandatory data protection training.

4.5 Staff will have attended training relating to the specific camera type they are monitoring or operating.

4.6 Cameras are all overt cameras.

4.7 Clear signs for fixed camera CCTV are located at points of access to the sites and other strategic locations to inform the public of the presence of the System and its ownership.

4.8 Staff operating BWV will have a badge indicating this. BWV cameras have a small screen which shows what is being recorded so people can see what is being captured by the cameras during use. BWV do record sound.

4.9 Vehicles carrying dash cams will be clearly marked with signage to indicate this. Dash cams do not record sound.

4.10 There will be some sound recording from the System from cameras where microphones are fitted, e.g. from Body Worn Video cameras and Security Mobile Dash cam. Fixed CCTV cameras do not record sound.

4.11 Recordings captured by the fixed cameras will be transmitted to a central dedicated Control Room on the main campus, where they will be recorded digitally for use in accordance with this Code.

4.12 Recordings captured by BWV will be initially stored on the device itself. On return to the Control Room they will be securely managed according to the BWV Standard Operating Procedure.

4.13 All System recordings will be automatically stored on one of four servers and retained for a period of no more than 30 days.

4.14 Once the 30-day period has been reached, the System will automatically record to the hard drive from the beginning and start overwriting the oldest images.

4.15 Although every effort has been made in the planning and design of the System, to give maximum effectiveness, it is not possible to guarantee that the System will detect every incident in the area of coverage.

5 The Control Room

5.1 Recordings captured by the System will be monitored in the Control Room, a self-contained and secure room on the main campus. The monitors cannot be seen from outside of the Control Room.

5.2 No unauthorised access to the Control Room will be allowed at any time. Daytime access to it will be strictly limited to the duty controller and a camera operator, authorised members of Senior Management and Police Officers who have requested access or been invited to attend. A list of University staff authorised for routine access to the Control Room, including Senior Management will be compiled and maintained.

5.3 Any other person may be authorised to enter the Control Room on a case-by-case basis. Authorisation is required and may only be given by the Director of Estates and Buildings, the Head of Transport & Security or his deputy. In their absence authority may also be granted by the Duty Manager or Security Controller. Each separate visit will require individual authorisation. In an emergency, when it is not practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter the Control Room.

5.4 Before granting access to the Control Room, Controllers must be satisfied as to the identity of any visitor and that the visitor has appropriate authorisation. All visitors will be required to complete and sign the Control Room Access Log, which shall include details of their name, their department or the organisation they represent, the person who granted authorisation for them (if

applicable), the reason for their visit and the date and times of the entry to and exit from the Control Room. The duty controller should also record details of persons admitted to the control room in an emergency.

5.5 At any time when visitors are in the control room, screens will be minimised to prevent accidental disclosure of data.

5.6 The University has an expectation that visitors do not disclose, to other people or organisations, anything heard, read or seen on any visit. All visitors will be informed of this expectation at the start of their visit. A notice setting out these terms as a condition of entry will be clearly displayed outside the point of entry.

5.7 All staff visitors will be expected to adhere to the Data Protection Policy and any issued guidelines.

6 Control Room Administration and Procedures

6.1 A daily log will be maintained in the Control Room and kept securely. Brief details of incidents, observations and points of interest will be noted, together with any consequential action taken and a corresponding incident number.

6.2 It is recognised that the recordings are sensitive and subject to data protection law. All copies will be handled in accordance with the University and police working procedures, which are designed to ensure the integrity of the System. The Head of Transport & Security will be responsible for the development of and compliance with the working procedures in the Control Room. A log will be kept for the purpose of recording the use of discs (where recordings have been downloaded for a specific purpose), their use by police and other agencies for evidential purposes.

7 Reviews

7.1 Recordings will only be reviewed in response to authorised requests for disclosure from the police, or with the authority of the Head of Transport & Security or their Deputies, and only in accordance with data protection law.

7.2 Copies of recorded data will only be made for the purpose of crime detection, evidence for prosecution, other judicial process, or for insurance purposes, or where required in response to a Subject Access Request (see 12.2.3 below).

8 Staff

8.1 All staff engaged in these duties and managers of the System will be vetted to industry standard of BS7858.

8.2 All University staff take mandatory data protection training, which is refreshed annually.

8.3 All staff will receive additional guidance and training on the need for sensitivity and security when handling images and recordings, and the requirement to appropriately protect data at all times.

8.4 The Head of Transport & Security will ensure that all staff are fully briefed and trained in the operational functions of the Control Room.

8.5 Training in the requirements of the law on data protection (GDPR and DPA2018) will be given to staff that are required to work in the Control Room.

8.6 Control Room training will comply with BS7499 where the standard is applicable.

9 Police Liaison

9.1 Surveillance cameras are an integral part of the University/Police partnership in improving campus safety. Regular contact will be maintained between the Head of Transport & Security and the Police University Liaison Officers to ensure that any problems are promptly dealt with or anticipated.

10 Recording

10.1 Images and footage captured on all cameras are recorded and stored as data. This data is held on one of the System's four servers.

10.2 Recordings are stored for a maximum of 30 days as already described in sections 4.13 and 4.14 above.

11 Monitoring Procedures

11.1 Camera Control

11.1.1 The Control Room is staffed 24hrs a day 7 days a week.

11.2 The control of the system will remain with the University but camera operations may be directed by police during an incident to:

11.2.1 Monitor potential public disorder or other major security situations

11.2.2 Assist in the detection of crime where the University has requested the Police's assistance.

11.2.3 Assist in the detection of crime where the Police have asked for the University's assistance.

11.2.4 Assist with a potential welfare issue identified by the Police and relating to individuals in the University grounds.

11.2.5 Facilitate the apprehension and prosecution of offenders in relation to public order.

11.3 On each occasion when the police obtain the University's assistance with their operations, a report setting out the time, date and details of the incident will be written by the Security and Transport Operations Manager and submitted to the Head Transport & Security. As noted in 10.4, we will obtain relevant documentation from police (and other bodies) if they require access to UEA personal data.

11.4 Where a major incident arises where life or property are threatened by criminal action, the police may take control of the CCTV Control Room for the period that the incident causes such a threat. In such instances a request to take control of the CCTV Control Room will be made formally by an Officer from a recognised agency, to the Director of Estates and Buildings. In the event of the Director of Estates and Buildings being unavailable the Head of Transport and Security may give permission for police to take control of the cameras. Where the Head of Transport and Security has given permission, the details of the police request and subsequent operation will be given in writing to the Director of Estates and Building as soon as possible. Access to personal data will only be granted where that is consistent with the obligations placed on the University by the GDPR and DPA2018.

11.5 Control of the cameras during such incidents will remain with Control Room staff who at times, where appropriate, may take direction from the Police.

12 Management of recordings (footage and still images): Procedures

12.1 Control and Management of recordings

12.1.1 All recordings (including footage and still images) belong to and remain the property of the University of East Anglia. Images are held in a Still Print log and Review Log and handling procedures are in place to ensure the integrity of the images held. All footage is held on servers owned and controlled by the UEA and is covered by the University's IT security policy. This policy ensures that all data is stored securely and will not be removed without permission and unless allowed by data protection law.

12.2 Access to recordings

12.2.1 We will obtain appropriate documentation from any organisation or individual requesting recordings or images and this will be shared with the University's Data Protection Officer and Information Compliance team, who maintain records of all such data sharing

12.2.2 In order to meet the requirements of the GDPR and the DPA2018, recordings will be kept secure recordings will not be shared with any

external party unless allowed by data protection law. The exceptions to this are:

12.2.3 Recordings are required in order to respond to a Subject Access Request. These are managed centrally by the Information Compliance team, who will liaise with the Security team to obtain requested data (see 7.2 above)

12.2.4 A request for viewing or copying of data made by the police or other body as described in GDPR and DPA2018.

12.2.5 Regular requests for a review of recordings in order to trace incidents that have been reported.

12.2.6 Immediate action relating to live incident e.g. immediate pursuit.

12.2.7 For major incidents that occur when the systems may be recording continuously.

12.2.8 Individual police officers seeking to review the footage within the Control Room. In accordance with s.29 request.

12.3 Viewing and Release of Recordings

12.3.1 If a request is made by the police or any other person to view or copy recorded images a record will be made of the request and any subsequent viewing or copying in the relevant CCTV Control Room Logs.

12.3.2 All recordings will be reviewed, and any images that are not relevant to the request will be removed using redaction software.

12.3.3 Any copies of required data will usually be transferred to DVD and subject to the same controls as images recorded on the system. Where data exceeds the capacity of a DVD it will be saved to a secure hard-drive and protected with encryption software.

12.3.4 If the images are copied and discs handed to the police or other authority the event will be noted in detail in the Digital CCTV Incident Management Log. As noted in 10.4, we will obtain relevant documentation from police (and other bodies) if they require access to UEA personal data.

12.3.5 Removal of discs will normally be for a period which will be long enough for the authorised third parties to view them or - where they may be required for evidence - no longer than the Court may require them. Discs that may be required by the police are to be retained securely

until it is confirmed they are required or no longer required for evidential purposes.

12.3.6 To ensure discs can be used in evidence, a comprehensive record of any handling of the disc will be maintained. Before leaving the Control Room the disc will be placed in a tamper proof, sealed evidence bag or sealed in a CD case with a tamper proof evidence seal. This is recorded in the Digital Evidence Receipt Book found within the Digital Evidence System.