

# Closed Circuit Television (CCTV) - code of practice

## UPR HS04 version 04.0

### Policies superseded by this document

This document replaces version 03.1 of UPR HS04, with effect from 12 December 2022.

### Summary of significant changes to the previous version

This document has been amended to bring legislative requirements information up to date and to reflect changes in organisational structures. A section on the use of Body Worn Video Cameras (BWVC) has also been added.

### Glossary

A glossary of approved University terminology can be found in [UPR GV08](#).

### Table of contents

1	Introduction .....	2
2	Definitions .....	2
3	Scope.....	2
4	Ownership and operation of the scheme .....	3
5	Principles.....	3
6	Purposes of the scheme.....	4
7	Key Objectives .....	4
8	Commercial and Collaborative use of the scheme.....	5
9	UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018	5
10	Use of recorded material and still images .....	6
11	Targeted Observations .....	6
12	Body Worn Video Cameras (BWVC) .....	6
13	Responsibilities of the owner of the scheme.....	7
14	Management of the scheme .....	7
15	Installation .....	7
15.2	University residences .....	7
15.3	Independent Observer .....	8
16	Monitoring and Evaluation .....	8
17	Arrangements for the amendment of this Code of Practice.....	8
17.1	Proposed changes to the purposes for which the scheme is operated will require approval in accordance with the requirements of section 5.2, iii.....	8
18	Subject Access.....	9

19	Procedures for the processing of requests for subject access to recorded material .	9
20	Breaches of this Code of Practice .....	9
20.2	Health and Safety .....	9
21	Complaints Procedure .....	10
22	How to obtain copies of this Code of Practice.....	10
23	General enquiries .....	10

---

## 1 Introduction

This Code of Practice was approved by the Finance and General Purposes Committee with effect from 3 March 2004<sup>1</sup> and has been amended subsequently by the Secretary and Registrar with effect from 1 September 2019.

## 2 Definitions

For the purposes of this Code of Practice, the following definitions will apply:

- i **‘University’**  
the University of Hertfordshire Higher Education Corporation;
- ii **‘scheme/system’**  
the University’s closed circuit television scheme;
- iii **‘Company’**:  
unless indicated otherwise, a company either wholly-owned by the Corporation or wholly-owned by a subsidiary company wholly-owned by the Corporation (Exemplas Holdings Limited is not a wholly-owned company);
- iv **‘Data Protection Officer’**  
the University’s Data Protection Officer.

## 3 Scope

This Code of Practice is binding on all employees and students of the University of Hertfordshire, all employees of the companies and applies also to all other persons who may, from time-to-time, and for whatever purpose, be present on University premises or the premises of its companies.

---

<sup>1</sup> Finance and General Purposes Committee Minute 659, 3 March 2004, refers.

## 4 Ownership and operation of the scheme

- 4.1 The closed-circuit television scheme which operates at the University of Hertfordshire is owned by the University of Hertfordshire Higher Education Corporation.
- 4.2 The University reserves the right to permit its scheme to be used for commercial purposes and in collaboration with those of other agencies provided that such use is consistent with the requirements of this Code of Practice (see section 8).
- 4.3 Unless the University has agreed alternative arrangements in cases where the scheme is used for commercial and/or collaborative purposes (see sections 4.2 and 8), all recorded material is owned by and the copyright of any recorded material is vested in, the University of Hertfordshire Higher Education Corporation.
- 4.4 The scheme is operated on behalf of the University by a contracted supplier of security services. The contractor provides security services to the University and the companies.
- 4.5 With effect from 20 March 2006, Contracted Security Operators will be required to be licensed under the Security Industry Authority scheme.

## 5 Principles

- 5.1 The lawful basis for processing personal data captured, i.e. images, with CCTV is for carrying out a specific task in the public interest; i.e. the detection, deterrence and prevention of crime; the provision of evidence for prosecuting bodies; the apprehension and prosecution of offenders and the safety of students, employees and the public.
- 5.2 The following principles will govern the operation of the scheme:
  - i the scheme will be operated fairly and lawfully and only for the purposes identified by the Board of Governors of the University (see section 6);
  - ii the scheme will be operated with due regard for the privacy of the individual;
  - iii any change to the purposes for which the scheme is operated (see section 6) will require the **prior** approval of the Vice-Chancellor and will be notified by the Secretary and Registrar, at the earliest opportunity, to the Board of Governors of the University and will be notified subsequently by University management to employees, students, clients, customers and visitors;
  - iv to ensure the security and integrity of the operating procedures for the scheme, these will be implemented and amended only with the prior consent of the Vice-Chancellor;
  - v the scheme will be regularly audited annually by a system auditor (normally the Head of Internal Audit (or nominee)).

## 6 Purposes of the scheme

The purposes of the scheme are as follows:

- i to assist in safeguarding the personal security and health and safety of students of the University; employees of the University and its companies; persons resident on University property; visitors to the University (including its clients and customers);
- ii to assist in safeguarding property belonging to students of the University; employees of the University and its companies; persons resident on University property; visitors to the University (including its clients and customers);
- iii to ensure the security of property belonging to the University and its companies;
- iv to aid the detection, deterrence and prevention of crime and in this regard to provide evidence for the Police and other bodies with prosecuting powers such as HM Revenue and Customs and the Health and Safety Executive;
- v where the scheme is used for commercial purposes or in collaboration with those of other agencies (see sections 4.2 and 8), to assist in safeguarding the personal security, health and safety and property of organisations and individuals in areas where the scheme is in operation; to aid the detection, deterrence and prevention of crime and in this regard to provide evidence for the Police and other bodies with prosecuting powers such as HM Revenue and Customs and the Health and Safety Executive.

## 7 Key Objectives

The key objectives of the scheme are as follows:

- i to detect, prevent and reduce the incidence of crime, in particular, criminal activity related to drugs and other illegal substances;
- ii to detect, prevent and reduce offences against the person;
- iii to prevent and to enable the University to respond effectively to harassment and bullying;
- iv to reduce instances of vandalism and other criminal damage;
- v to reduce theft of property belonging to individuals, to the University and to its companies;
- vi to improve the speed with which the University is able to alert the Police to unlawful activity.

## 8 Commercial and Collaborative use of the scheme

Proposals for use of the scheme for commercial and/or collaborative purposes (see section 4.2) will require the prior written consent of the Vice-Chancellor (or nominee) who must be satisfied that the arrangements for such use are consistent with the requirements of this Code of Practice, in particular that appropriate arrangements are in place concerning the use of recorded material and still images; the fulfilment of the responsibilities of the University as the owner of the scheme; management of the scheme; installation and use of the scheme; monitoring and evaluation; subject access and complaints and that these arrangements are the subject of a written agreement between the parties.

## 9 UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018

- 9.1 The University and its companies include the scheme within the Notifications ('registration of data systems') which they are required to make under the terms of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
- 9.2 The scheme will be operated in accordance with the guidelines set out in the 'CCTV 'Amended' Surveillance Camera Code of Practice 2022 (Code of Practice)' published by the office of Biometrics and Surveillance Camera Commissioner (BSCC). In particular, the University system will follow the 12 Guiding Principles as directed by the BSCC. In summary, the UH CCTV system including BWVC will remain compliant with the following (extracted from the 12 Principles):
- i recorded material shall be obtained, held and processed fairly, lawfully and in accordance with the ODPC Code;
  - ii recorded material shall not be used or disclosed for a purpose or in a manner which is incompatible with the ODPC Code and will not be transferred to countries without adequate data protection legislation;
  - iii recorded material shall be adequate, relevant and not excessive in relation to the purposes set out in this Code of Practice;
  - iv where recorded material is retained for any of the purposes set out in this Code of Practice that material shall not be kept for longer than is necessary for the purpose for which it is being retained (material will normally be destroyed after **30** days);
  - v recorded material will be stored securely. Access to it will be permitted strictly in accordance with this Code of Practice and the Closed Circuit Television Operating Procedures determined by the University and operated on its behalf by the security contractor.
- 9.3 The University will ensure that appropriate security measures are taken to prevent unauthorised access to, or alteration, disclosure or destruction of, recorded material and to prevent accidental loss or destruction of such material.

- 9.4 Recorded material will not be sold or used for commercial purposes or for the provision of entertainment or to provide information or material for research purposes.

## **10 Use of recorded material and still images**

- 10.1 Still images will be generated from recordings made by the system only where these are required for evidential purposes by the Police or other bodies with prosecuting powers or by the University.
- 10.2 Unless required to do so by a court of law and only where the request is compatible with the purposes of the scheme:
- a recordings made by the system and/or still images generated from such recordings will not normally be made available by the University to individuals wishing to use these as evidence in a civil proceedings;
  - b recordings made by the system and/or still images will not be disclosed to third parties.
- 10.3 The University of Hertfordshire reserves the right to use a recording made by the system and/or still images generated from such a recording as evidence in any civil proceedings brought by or against the University of Hertfordshire Higher Education Corporation or any of its companies.
- 10.4 The University of Hertfordshire reserves the right to use a recording made by the system and/or still images generated from such recordings as evidence in internal grievance/complaints investigations and/or in disciplinary investigations involving students or employees of the University of Hertfordshire or employees of any of its companies provided such use is consistent with the purposes of the scheme specified in section 6.
- 10.5 Other than where it is required for a reason consistent with the purposes of the scheme and this Code of Practice, recorded material will be retained for a period of **30** days. In storing recorded material, reasonable efforts will be made to maintain the quality of the images, insofar as possible, to ensure accuracy in the images.

## **11 Targeted Observations**

For good reasons and in compliance with the declared purposes and key objectives of the scheme and the protocols governing the provision of evidence, the system may be used for targeted observation.

## **12 Body Worn Video Cameras (BWVC)**

- 12.1 The use of Body Worn Video Cameras (BWVC) has been approved by the University. The University Security team use BWVC to improve the safety of staff, students, and visitors of the University. Evidence indicates that the use of video recording devices may reduce the incidence of aggression and violence whilst also providing greater transparency and enabling increased scrutiny for any subsequent actions taken in response to such occurrences.

- 12.2 BWVC should not be used in private spaces, such as toilets, changing rooms, student personal accommodation unless a clear verbal warning is issued by the officer wearing the device prior to the commencement of recording.
- 12.3 Individuals are likely to have a strong expectation of privacy, in places not generally open to the public, such as their private residence, especially at a time of day when occupants are likely to be in bed. Clear justification of the necessity to use BWV will be required in such circumstances.

## **13 Responsibilities of the owner of the scheme**

It is the responsibility of the University, as the owner of the scheme:

- a to ensure compliance with this Code of Practice;
- b to ensure compliance with relevant requirements of the Security Industry Authority;
- c to approve the operating procedures for the scheme;
- d to ensure that these operating procedures have been complied with;
- e to ensure that the purposes and objectives of the scheme are not exceeded;
- f to notify persons entering the University that a closed-circuit television scheme is in operation; and
- g to provide copies of this Code of Practice when requested to do so.

## **14 Management of the scheme**

- 14.1 The scheme is managed, on a day-to-day basis, by the Head of Security & Resilience and the Security Manager-Security Systems.
- 14.2 The Vice-Chancellor (or their nominee designated for this purposes), is the officer of the University designated as having overall responsibility for security matters.
- 14.3 Access to the University's system, to the Control Room and access to and the release of images and recordings made by the system, will be strictly in accordance with the operating procedures established by University management (see section 12, c).

## **15 Installation**

- 15.1 The installation of the scheme will be appropriate to its purposes and to the requirements of this Code of Practice.

### **15.2 University residences**

When installing cameras in residential areas, the University will have regard for the privacy of residents and bona fide visitors to University residences.

### **15.3 Independent Observer**

- i The Director of Estates will nominate a member of staff of appropriate seniority to act as Independent Observer.
- ii In the presence of either the Head of Security & Resilience or the Security Manager-Security Systems, the Independent Observer will, at intervals of **30** days, review the use made of cameras installed in residential areas to ensure that the privacy of residents has not been infringed unreasonably.
- iii The Independent Observer shall have full access to material recorded by cameras installed in residential areas.

(In addition to the regular reviews made by the Independent Observer, the Head of Security & Resilience or the Security Manager-Security Systems will undertake reviews at other times.)

## **16 Monitoring and Evaluation**

- 16.1 This Code of Practice, its operation and the operation of the University's closed-circuit television scheme will be reviewed annually by the Audit Committee of the University's Board of Governors.
- 16.2 To enable this process, the Secretary and Registrar will appoint a system auditor who will monitor the operation of this Code of Practice and the operating procedures for the scheme to ensure compliance with legal obligations and the provisions of the Amended' Surveillance Camera Code of Practice 2022 (Code of Practice).
- 16.3 The Secretary and Registrar will also make an Annual Report to the Audit Committee of the Board of Governors. Those elements of the Annual Report which relate to the operation of this Code of Practice will normally be a matter of public record.

## **17 Arrangements for the amendment of this Code of Practice**

- 17.1 Proposed changes to the purposes for which the scheme is operated will require approval in accordance with the requirements of section 5.2, iii.
- 17.2 Proposed changes to the arrangements for the monitoring and evaluation of this Code of Practice will require the prior approval of the Audit Committee.
- 17.3 The Vice-Chancellor may approve other amendments to this Code of Practice for the proper administration of the University and the scheme.



## **18 Subject Access**

- 18.1 Personal Subject access to material recorded via the system will be permitted only by the Data Protection Officer in response to a formal request from the subject (called a 'Subject Access Request'). Data Subjects requesting access to CCTV material must provide the Data Protection Officer with a recent photograph of themselves and must also indicate the date, approximate time and the location at which the requested CCTV images were recorded.
- 18.2 Individuals wishing to access recorded material of which they are the subject must be referred to the University's Data Protection Officer.
- 18.3 Other than in exceptional circumstances, the recorded material made available to the data subject will relate only to the data subject. Where the material unavoidably identifies another individual, that individual must either have given written consent to the disclosure of the material or their image must have been hidden prior to the material being made available to the data subject.

## **19 Procedures for the processing of requests for subject access to recorded material**

- 19.1 Any member of the University's staff or employee of a company or of the security contractor who receives a personal subject access request must forward it immediately to the Data Protection Officer.
- 19.2 To allow the required data to be identified and to enable the request to be processed, individuals are requested to complete and return to the Data Protection Officer the 'Subject Access Request Form' which they will supply to them. The requester will be required to provide appropriate ID for verification purposes.
- 19.3 It should be noted that, pursuant to the 2018 Act, no action will be taken on the request until the Data Protection Officer has received the required request and identification documentation. The Data Protection Officer will normally respond to the request within **30** days of the day on which the request and ID was received provided that they have sufficient information to identify the data subject and locate the recorded material which is sought.

## **20 Breaches of this Code of Practice**

- 20.1 The University reserves the right to take disciplinary action against any employee or student who breaches this Code of Practice in accordance with the University's disciplinary procedures.

### **20.2 Health and Safety**

A purpose of the University's scheme is that it should be used to assist in safeguarding the health and safety of students, employees, residents, and visitors (see section 6, i). It should be noted that intentional or reckless interference with any part of the scheme (including cameras), may be a criminal offence and will be regarded as a breach of discipline.

## 21 Complaints Procedure

- 21.1 Grievances and complaints by staff and students concerning the operation of the University's closed-circuit television scheme may be progressed through the relevant University grievance/complaints procedures which are published on-line at the following location (see UPR HR03<sup>2</sup> and UPR SA16<sup>3</sup>):

<https://www.herts.ac.uk/about-us/governance/university-policies-and-regulations-uprs/uprs>

Copies of these procedures may also be obtained on request from the Secretary and Registrar.

- 21.2 Other individuals should write to the Secretary and Registrar, providing an account of their grievance or complaint. The Secretary and Registrar will conduct an investigation and respond on behalf of the University, in writing, within twenty (20) working days of the receipt of the written account or as soon as possible thereafter.

## 22 How to obtain copies of this Code of Practice

- 22.1 **This Code of Practice is published on-line at the following open-access location:**

<https://www.herts.ac.uk/about-us/governance/university-policies-and-regulations-uprs/uprs/health-safety-and-security>

- 22.2 Copies of this Code of Practice are available on request from:

- i Governance Services;
- ii **the Reception Desks at each of the University's campuses.**

## 23 General enquiries

Enquiries concerning this Code of Practice and/or the operation of the University's scheme should be directed to the Secretary and Registrar, University of Hertfordshire, Hatfield, Herts AL10 9AB.

Sharon Harrison-Barker  
Secretary and Registrar  
Signed: **12 December 2022**

### Alternative format

If you need this document in an alternative format, please email us at [governanceservices@herts.ac.uk](mailto:governanceservices@herts.ac.uk) or telephone us on +44 (0)1707 28 6006.

---

<sup>2</sup> UPR HR03 'Staff Grievance Policy'  
<sup>3</sup> UPR SA16 'Student and Applicant Complaints'