University of Reading

CCTV Code of Practice

1 Scope

The University of Reading has installed a comprehensive, image-only CCTV surveillance system across the Whiteknights, Greenlands and London Road campuses. Automatic Number Plate Recognition (ANPR) is always used at the main entrances and exits from Whiteknights and Greenland campuses. References to CCTV throughout this document also apply to ANPR. This code of practice covers CCTV recording across Whiteknights Campus, London Road Campus, Greenlands Campus, Thames Valley Science Park, Earley Gate, Bulmershe Pavilion and all University Halls of Residence. All images will be monitored by the staff from Security in the Control Rooms on Whiteknights Campus, London Road and Greenlands

Cameras located within buildings will also be monitored by Security Control. All staff operating the CCTV system will do so in compliance with the University's policies and guidance on Data Protection available at:
http://www.reading.ac.uk/internal/imps/policiesdocs/imps-policies.aspx

This Code of Practice (Code) has been prepared for managers and the operators of the CCTV system to ensure that CCTV operations are consistent with the obligations on the University imposed by the General Data Protection Regulation 2016, the Data Protection Act 2018 and codes of practice and guidance issued by the Information and Surveillance Camera Commissioners. Its purposes are listed below in full. The Code is published at: **www.reading.ac.uk/cctv**.

2 Purposes

2.1 CCTV has been installed by the University for the following purposes:

- to assist in the prevention and detection of crime;
- to facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order;
- to help ensure public safety;
- to assist with the identification of actions that may result in disciplinary proceedings against staff or students;
- to monitor and assist with traffic management issues on campuses listed in the Scope;
- to reduce the fear of crime and to reassure students, staff and visitors.

3 System

3.1 Scope

The CCTV system encompasses the University's campuses and Halls. It will also encompass all other CCTV images that, in due course, are added to the system and monitored in the 24 hour Control Room. References in this code to the "CCTV system" or "system" should be read accordingly.

3.2 Operation

The CCTV system operates throughout the year for 24 hours a day.

3.3 Presence and ownership of CCTV

The public is made aware of the presence and its ownership of the CCTV system by appropriate signage. Signage will always be displayed in prominent areas and include the contact details of the Data Controller.

3.4 Privacy

To respect privacy, wherever practicable, the cameras are prevented from focusing or dwelling on domestic accommodation and this will be demonstrated on request to local residents. Where domestic areas such as gardens about those areas which are intended to be covered by the scheme the Security Services Manager (or his/her nominee) will consult with the owners of the domestic area to discuss what images may be recorded. Where it is not practicable to prevent the cameras from focusing or dwelling on such areas, or where domestic areas are intended to be covered, training will be given to the system operators to ensure that they are made aware of the policies, procedures and requirements in these instances, which includes the pixelating of more privacy intrusive areas where deemed necessary. In circumstances where there is a legitimate need for CCTV that may have any additional privacy impact on individuals, a Data Protection Impact Assessment will be conducted under the supervision of the University Data Protection Officer.

3.5 Recordings, storage and access

Images captured on camera are recorded on a digital hard drive. While local managers will have access to local recorders, persons monitoring the images at locations other than the Control Room will not be permitted to record those images or to have access to archived images. Any images recorded in these systems will be held centrally and managed by the Security Services Manager.

3.6 Data Controllers

For the purposes of the General Data Protection Regulation 2016 and the Data Protection Act 2018, the Data Controller is the University of Reading and it is legally responsible for the management and maintenance of the CCTV system.

3.7 Contracted supplies

Any contracted suppliers used in connection with the provision of CCTV, who are acting as data processors will work in accordance with a written contract, will only process data on the instruction of the University, with defined responsibilities and adequate provisions for security and training of those personnel with access to images.

4 Security of CCTV data

4.1 Captured images

Images captured by the system will be monitored in the Control Room, which is a self-contained, secure and restricted area.

4.2 Authorised access

Other than emergencies, no unauthorised access to the Control Room is allowed at any time. Normal access is strictly limited to authorised persons, including:

- Security Staff and their Line Managers
- Management staff with remote viewing monitors
- Police officers
- Data Protection Officer
- Other statutory officers, e.g. Health & Safety Executive officers
- Authorised employees of contractual suppliers in place for CCTV

4.3 Access control system

A list of persons authorised for routine access to the Control Room will be held by the access control system and maintained by contractual suppliers.

4.4 Access procedures

Before granting access to the Control Room, controllers must satisfy themselves of the identity of any visitor and ensure that the visitor has the appropriate authorisation.

4.5 Logging access

All visitors will be logged, including details of their name, the department or the organisation they represent, the person who granted authorisation for the visit (if applicable) and the times of their entry to and exit from the Control Room.

5 Control room administration and procedures

5.1 Incident log

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

5.2 Personal data

CCTV images may be personal data and therefore fall within the scope of the General Data Protection Regulation 2016, the Data Protection Act 2018 and all applicable privacy laws. All processing of personal data will be done in accordance with University's policy on data protection http://www.reading.ac.uk/internal/imps/policiesdocs/imps-policies.aspx

5.3 Responsibility for procedures

The Security Services Manager will be responsible for the development of and compliance with the working procedures in the Control Room and Information Asset Owner for CCTV images.

5.4 Recorded images

Recorded images will only be reviewed with the authority of the Security Services Manager (or nominee).

5.5 Copies of recorded images

Copies of tapes or digital images will only be made for the purposes set out in 1.1 or otherwise required by law.

6 Staff

6.1 Staff, Training and Further Guidance

All staff involved in the operation of the CCTV system will be required to have read and understood this Code. Only authorised members of staff will have access to CCTV images. The Security Services Manager will ensure that all staff involved with the operation of CCTV are trained in respect of all operational, legal and administrative functions arising out of CCTV operations, including mandatory University information compliance training.

Further Guidance on Data Protection Act are provided for staff at **www.reading.ac.uk/data_protection.**

7 Recording, handling and retention

7.1 Digital recording

The Control Room system and local systems are supported by digital hard drive recording facilities. The digital recording system is capable of retrieving images to a dedicated server or to an external device.

7.2 Identifying and recording discs and images

Discs, still photographs and printed images will be uniquely identified. All activities relating to each disc - for instance, the date and time of recording, purpose of viewing, the copies taken, whether discs are retained - will be recorded for evidence. For images recorded digitally, all identifying retrieval dates and times will be recorded.

7.3 Logs

A log will be maintained within the Control Room containing details as to the dates when the tape/disk/photograph/print was introduced into the system or created and when it was disposed of. An entry will be made in the log 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.

7.4 Retention

Unless required for evidential purposes or the investigation of crime or otherwise required by law, recorded images will routinely be retained for no longer than 28 days from the date of recording.

7.5 Accuracy and Quality

Features such as the location of the camera and/or date and time reference will be accurate. The quality of images shall be appropriate for the purposes stated in 2 above.

7.6 Erasure and Disposal

At the end of their useful life all images on discs will be erased and securely disposed of as confidential waste. All still photographs and hard copy prints also will be securely disposed of as confidential waste. Such erasure and disposal will be logged by the Control Room. Disposal will be in line with University guidance.

7.7 Software updates and maintenance of systems

All CCTV software and systems will be kept up to date and maintained to ensure security and compliance with relevant legislation.

8 Procedures

8.1 Requests to view or copy images

Requests to view or copy CCTV images will be considered on a case-by-case basis by the Security Services Manager (or nominee). If access is denied the reasons should be documented in the Control Room.

8.2 Requests from the Police or law enforcement agencies

Requests from the Police or other law enforcement agencies may arise for a number of purposes, including:

- For the prevention or detection of a crime;
- For the apprehension or prosecution of offenders;
- For the assessment or collection of any tax or duty or any imposition of a similar nature;
- For immediate action relating to live incidents, e.g. an immediate pursuit;
- For the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
- Is otherwise necessary for the purposes of establishing, exercising or defending legal rights;
- For major incidents that may occur.

8.3 Guidance on how to deal with requests from the Police or law enforcement agencies

Clear guidance for staff on how to deal with requests from the Police and other law enforcement agencies can be obtained from the Data Protection Officer. In the first instance, all requests for CCTV from law enforcement agencies should be addressed to the Security Control room.

Law enforcement agencies should provide appropriately authorised data disclosure forms which establish their identity and the purposes for which they require the disclosure. Staff should follow guidance issued by Data Protection Officer and the Data Sharing Agreement with TVP, RUSU and UPP.

8.4 Third party access

Access by other third parties to recorded images will be dealt with under Information Compliance laws and should be addressed to **imps@reading.ac.uk**.

8.5 Access to recorded images

Access to recorded images will be restricted to only those staff concerned with the purposes set out in 1.1 and will be documented by the Control Room.

8.6 Security of recorded images

It is the responsibility of the Security Services Manager to ensure that the method used to disclose images is secure and complies with University policy on encryption: www.reading.ac.uk/encryption-policy

8.7 Accessing personal data

Individuals have a right to request access to their own personal data which can include CCTV images. Individuals wishing to access their personal information contained within CCTV images should follow the procedure given at: **www.reading.ac.uk/accessing-personal-data**

The method of disclosure shall be secure.

8.8 Third party personal data

Where third parties are identifiable, third party personal data may be anonymised or redacted.

9 Complaints and contacts

9.1 Complaints

The Security Services Manager is responsible for the operation of the CCTV system, and compliance with this Code. Any concerns in respect of the system's use or regarding compliance with this Code should be addressed to the Security Services Manager.

9.2 Contacts:

Reading University

Security Services Manager	0118 378 6967	security@reading.ac.uk
Security Services Control Room	0118 378 7799	security@reading.ac.uk
Campus Services Director	0118 378 6246	campus-services@reading.ac.uk
Data Protection Officer	0118 378 8981	imps@reading.ac.uk

Document detail	Previous Version	Current Version
Author	**Nigel Courtenay**	**Security Services, Technical Supervisor.**
Draft date	**16th February 2015**	**7th February 2019**
Custodian	**Nigel Courtenay**	**Security Services, Technical Supervisor**
Version no.	**5**	**6**
Review date	**February 2017**	**February 2022**
Approving body/committee	**Estates & Facilities Committee**	**Estates Committee Minute Reference 19/16**
Date approved	**5th March 2015**	**28th February 2019**