Professional Services
Directorate of Estates, Facilities and Capital Development

Closed Circuit Television (CCTV) Policy

Author Names	Kevin Rowan, Head of Campus Security Ben Goddard, Senior Information Governance Officer
Reviewed By	Stephen Bloye, Deputy Director of Estates, Facilities and Capital Development
Final Approval Date	April 2020
Final Approval	Andrew Fallon, Director of Estates, Facilities and Capital Development
Review Date	August 2023
File Location	mmu.ac.uk/policy

Contents

1. Security Strategy

Manchester Metropolitan University's Security Strategy provides a framework for managing the security of the campus, staff, students, and visitors. The strategy will minimise risks and ensure the University has systems, policies, procedures and measures in place so that all users of the campus can conduct their activities in a safe and secure environment.

2. Policy Statement

This Policy describes the Close Circuit Television (CCTV) system in use at Manchester Metropolitan University and how it is managed and operated in compliance with the current legislation - General Data Protection Regulation (GDPR) and includes the principles governing the processing of personal data as set out in in this policy.

It also informs of Manchester Metropolitan's compliance with Data Protection Legislation, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, the Private Security Industry Act 2001, the Protection of Freedoms Act 2012, the Surveillance Camera Code of Practice 2013, the Counterterrorism and Security Act 2015, and the University's Data Protection Policy. Manchester Met seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors, contractors, its property, and premises.

Manchester Metropolitan University prioritises the security, wellbeing, comfort and safety of all students, staff, visitors, contractors on campus and utilises and its CCTV to:

- Support its objective to create a safe and welcoming campus.
- Assist in the prevention, investigation and detection of crime.
- Assist in the apprehension and prosecution of offenders, using recorded images as evidence in criminal investigations.
- Support investigations of breaches of code of conduct and policies by staff, students and contractors and where relevant and appropriate investigating complaints.

This policy will be reviewed annually by the Head of Campus Security to ensure compliance to current and relevant legislation.

3. CCTV

CCTV at Manchester Met comprises a number of cameras, installed at strategic locations, which can be monitored 24hours/365 days a year. Cameras are mostly colour and use either pan tilt and zoom or static facilities. There is no capacity within the CCTV Scheme for CCTV to be used, or adapted for use, to record sound and conversations.

The University's CCTV Scheme may result in the processing of images from which specific individuals may be identified, and which fall within the definition of 'personal data' in line with the UK General Data Protection Regulation (UK GDPR).

The purpose of the use of CCTV at Manchester Metropolitan is to~~o~~:

- Help ensure a safer environment and reduce fear of crime.
- Facilitate the prevention and detection of crime.
- Assist with the apprehension and prosecution of offenders.
- Assist with the investigation of potential breaches of university regulations which may result in disciplinary proceedings against students or staff.
- Assist the University with traffic management and car park access.

The Scheme will not routinely be used for workforce monitoring or for covert monitoring however, the University reserves the right to use CCTV for overt and/or covert monitoring in exceptional circumstances, as part of a specific investigation (such as to prevent or detect criminal activity or equivalent malpractice), with approval from the Director of Estates, Facilities and Capital Development (EFCD) and the University's Legal Department.

The CCTV Scheme cannot prevent or detect every incident which occurs within the University or the areas covered by the scheme.

4. Roles and Responsibilities

The University is responsible for CCTV on campus and is the registered controller for the personal data processed under the scheme.

The Head of Campus Security is responsible for ensuring that the images captured on CCTV equipment are retained and deleted in compliance with the University's published retention and disposal schedule.

The Head of Campus Security is responsible for the overall management and operation of the CCTV Scheme, including the training and licensing (where appropriate) of Campus Security staff and CCTV Operators.

No other CCTV installation or use of CCTV by University employees is permitted without the authority of the Head of Campus Security.

All employees (including temporary and contract staff) who are responsible for implementing, managing, operating, or using the CCTV Scheme must:

- Have authorisation to use Manchester Metropolitan University's CCTV from the Head of Campus Security in accordance with this Policy and the applicable data protection legislation.
- Operate with respect for the privacy of individuals.
- Use CCTV for the purposes described within this Policy and for no other purpose.

Failure to comply with this policy may result in disciplinary action and/or criminal liability.

5. Impact Assessments

Camera sites and locations are determined appropriately to respect privacy. Wherever practicable cameras are restricted to areas which are intended to be monitored and exclude views of areas that are not of interest. Cameras are not sited to focus on private or residential areas. Where cameras unavoidably overlook residential areas, privacy screens will be installed.

A Data Protection Impact Assessment shall be carried out prior to introducing a new CCTV scheme or where changes are made to the current scheme which are likely to significantly affect the rights and freedoms of the individual.

6. Signage and Transparency

The University notifies individuals whose images may be captured by the CCTV Scheme of the use of CCTV and its purposes, by means of this policy and by prominently placed signage at building entrances and CCTV monitored zones. Signs are legible, visible, appropriately sized, relevant to the location, confirm that the University operates the CCTV and informs of the purpose of the CCTV Scheme and who to contact.

The University CCTV Privacy Notice is available at:
mmu.ac.uk/data-protection/privacy-notices

7. Technology

Manchester Metropolitan University's CCTV technology and software is appropriate to ensure that images are adequate for the purpose for which they are obtained. For crime detection and prevention purposes, images are sufficiently clear to be able to identify individuals and to be used in evidence. The Scheme complies with the following quality controls:

- CCTV equipment is checked, maintained, and cleaned regularly to ensure it functions properly and clear images are recorded. Records of maintenance work are retained.
- Where copies of recordings are required (e.g., for investigations/evidence) quality and encrypted data storage devices and DVD-Rs are used (once only).
- CCTV images are retained for standard maximum retention period of 30 days, after which the images will be securely destroyed. Occasionally, images may be retained for longer for investigating a crime or internal disciplinary investigation.
- CCTV images are kept securely in a controlled access area.
- Data gathered from CCTV cameras shall be transmitted and stored in a way that maintains integrity, availability, and confidentiality, in order to ensure that the rights of individuals whose images are captured by the CCTV scheme are protected. CCTV images are kept

securely in a controlled access area, CCTV will be monitored and reviewed by authorised members of staff with a legitimate reason to do so.

- The CCTV Scheme does not routinely include areas requiring a heightened expectation of privacy (such as changing rooms or toilet areas).
- All employees and workers responsible for managing, operating, or otherwise using CCTV are trained in conjunction with this Policy.
- Manchester Metropolitan will endeavor to ensure that all CCTV is functioning and operating normally, and images are stored and available on request. This will be dependent on system functionality at the time of request.
- Body worn video cameras (BWVC) may be used by University Campus Security staff. Campus Security staff members will activate cameras where there is a recognised requirement to record footage and will declare to individuals captured that video and audio recording will take place. Body worn video is downloaded daily onto secure storage at the end of each shift (or before such time), at which point it is removed from the device.
- The CCTV scheme also applies to the University's use of Automatic Number Plate Recognition (ANPR) which is used to assist in car parking management.

8. Disclosure of Images and Subject Access Requests

Recorded images, if sufficiently clear, are the personal data of the individuals (Data Subjects) whose images have been recorded by the CCTV system. Data Subjects have a right of access to the personal data under the UK GDPR. They also have other rights under the UK GDPR, including the right to have their personal data erased, rectified, to restrict processing and to object to the processing of their personal data. These rights apply in certain circumstances, for example according to the lawful basis utilised by the University.

Data Subjects can exercise their rights by submitting a request to the University.

On receipt of a request, the University will liaise with the Head of Campus Security regarding compliance with the request, and subject to the UK GDPR will communicate the decision without undue delay and at the latest within one month of receiving the request from the Data Subject.

Access and disclosure of CCTV images is restricted to ensure respect for the privacy of individuals and that the value of images required for evidence is maintained. Third party requests for access will usually only be considered in line with the UK GDPR from:

- Legal representative of the Data Subject.
- Law enforcement agencies including the Police.
- Disclosure required by law or made in connection with legal proceedings.
- University staff members responsible for student and staff disciplinary complaints and investigations and related proceedings.

CCTV images may be released where the disclosure is necessary for the purposes for which the images were recorded or required by law. Exceptionally, disclosure may be granted in other

circumstances, such as for legal proceedings or insurance investigations.

The University retains discretion to refuse any request for information unless there is an overriding legal obligation. The CCTV privacy notice and subject access webpage contain information on how data subjects are able to exercise their right of access. The University's information requests webpage provides further details to third parties who would like to make a request for information. A record of all requests for disclosure will be retained.

9. Complaints

Complaints or information requests relating to the CCTV system should be made to the Head of Security. A complaint will be responded to within a month following the date of its receipt. Records of all complaints and any follow-up action will be maintained by the relevant office. Complaints in relation to the release of images should be addressed to the University as soon as possible, no later than 30 days from the date of the event.

Complaints should be raised in the first instance to:

Campus Security Duty Manager:
Tel: 0161 247 6656
Email: SecurityDutyManager@mmu.ac.uk

Appendix A: Privacy Notice for University Use of CCTV

Privacy Notice for University Use of CCTV

This Privacy Notice explains who we are, how and why we collect and use personal information about you if you appear on a University CCTV device, what personal data is collected and held about you, our purposes and lawful bases for processing, details of who we share your personal data with, relevant retention periods, and how you can exercise your data subject rights.

Please read this notice to understand our practices and if you have any questions, please contact us using the contact details provided below.

Who we are and how we capture personal data

Throughout this notice, "University", "we", "our" and "us" refer to the Manchester Metropolitan University, an exempt charity under Schedule 2 to the Charities Act 1993 (amended by the Charities Act 2011). The University is the Controller in respect of the personal data held about you as an external examiner.

The University is registered as a Controller with the Information Commissioner's Office (ICO). We manage personal data in accordance with the General Data Protection Regulation (GDPR) and the University's Data Protection Policy.

Our CCTV monitors various locations across the campus 24 hours a day, every day of the year. These locations are carefully selected to fulfil the purposes of the processing, while still having due regard to the privacy of the data subjects. The CCTV images are monitored and reviewed by authorized University staff where it is reasonably necessary to fulfil the purposes outlined in this notice and within the University's CCTV policy.

Cameras are not placed in areas that have an expectation of privacy (such as in changing rooms) except in exceptional circumstances, where a thorough assessment has been conducted and the University has very serious concerns.

CCTV will not normally be used for routine workforce monitoring or for covert monitoring; however, the University reserves the right to use CCTV for overt and/or covert monitoring in exceptional circumstances, as part of a specific investigation (such as to prevent or detect criminal activity or equivalent malpractice), with approval from the Director of Estates, Facilities and Capital Development (EFCD) and the Legal Department.

The University conducts the following types of recording:

- Fixed camera CCTV around the Manchester Metropolitan campus
- Use of body worn cameras by designated Campus Security staff
- Automatic Number Plate Recognition in certain parking facilities

Body worn cameras may be used by the University's Campus Security staff. Security staff members will activate cameras where there is a recognised requirement to record footage and will declare to individuals captured that video and audio recording will take place.

The personal data we process

We collect and process recorded images through the use of our CCTV system. We do not collect audio data except through use of the body worn cameras. Images including vehicles and individuals are captured at a level of definition considered to be necessary for the intended purpose such as, for reasons identification, health and safety or traffic management.

Camera sites and locations are determined appropriately and, in order to respect privacy, wherever practicable cameras are restricted to monitor only those areas which are intended to be monitored, excluding views of areas that are not of interest. Cameras are not sited to focus on private residential areas. Where cameras unavoidably overlook residential areas, privacy screens will be fitted.

The CCTV system captures images of people and their activity, which may include special categories of personal data, as defined by the General Data Protection Regulation. This may include personal data pertaining to an individual's racial or ethnic origin, data concerning health or data concerning sex life or sexual orientation of an individual. The information may also include details relating to the commission of offences.

The purposes of the processing

<table>
<tr><th>Your information will enable us to:</th><th>Lawful basis for the processing:</th></tr>
<tr><td>Help ensure a safer environment for students, staff, visitors, and members of the public and reduce fear of crime.</td><td rowspan="3">For personal data:
Processing is necessary for the performance of a task carried out in the public interest.

In cases of special category data:
Processing is necessary in the substantial public interest, specifically for the purposes of the prevention or detection of an unlawful act.</td></tr>
<tr><td>To assist law enforcement agencies and to facilitate the prevention and detection of crime, including the identification, apprehension, and prosecution of offenders. This includes the protection of buildings and assets from damage, disruption, vandalism
and other crime.</td></tr>
<tr><td>Assist with the investigation of potential breaches of university regulations and/or actions which may result in disciplinary proceedings against students or staff.</td></tr>
<tr><td>Assist the University with traffic management and car park access.</td><td>Processing is necessary for the purposes of the legitimate interests pursued by the University.</td></tr>
</table>

To assist in the defense of any civil litigation, including employment tribunal proceedings which involve Manchester Metropolitan University or other relevant individuals.	For personal data: Processing is necessary for the performance of a task carried out in the public interest. In cases of special category data: Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

The recipients or categories of recipients of the personal data

We may disclose personal data about you to the following third parties:

- Law enforcement agencies for the purposes of the prevention and detection of crime.
- Other relevant organisations such as health care agencies or the emergency services for safeguarding or public protection reasons.

The University conducts relevant assessments to ensure lawfulness, necessity, and proportionality prior to sharing any information captured by the CCTV system with external organisations.

Data retention

Your personal data will only be retained for as long as it is necessary in accordance with the University's Retention and Disposal Schedule. Specifically, we will retain CCTV images as follows:

Record	Retention period
Fixed camera CCTV footage and body worn camera footage	30 days

Occasionally, images may be retained for longer to meet the purposes for which the images were taken, eg, for investigating a crime or disciplinary matter.

Your rights in respect of the processing

The GDPR provides data subjects with the following data subject rights:

- The right to be informed – this privacy notice assists with fulfilling these obligations
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

Please note, that these rights apply in certain circumstances, for example according to the lawful basis utilised by the University. The right of access to personal information held about you exists in order to be aware of, and verify, the lawfulness of the processing. Please use the contact information below to exercise these rights.

Contacting us

For questions or concerns about this Privacy Notice, or our use of your personal information, please contact the security control room on 0161 247 6656 or email SecurityDutyManager@mmu.ac.uk in the first instance.

Our Data Protection Officer can also be contacted as follows:

By email: DataProtection@mmu.ac.uk
By phone: 0161 247 3884 or by writing to:

Data Protection Officer
Legal Services
All Saints Building
Manchester Metropolitan University
Manchester, M15 6BH

Right to lodge a complaint with the supervisory authority

You have the right to lodge a complaint with the Information Commissioner's Office (ICO) as the supervisory authority in respect of the processing of your personal data. We would encourage you to use our internal complaints procedure through our initial contact and the University Data Protection Officer, prior to contacting the ICO. Please contact:

By email: casework@ico.org.uk
By phone: 0303 123 1113.

For any further contact information please see: ico.org.uk/global/contact-us

Updates to this privacy notice

We may update this privacy notice from time to time in response to changing legal, technical or business developments. When we update our privacy notice, we will take appropriate measures to inform you, consistent with the significance of the changes we make.