Manchester Metropolitan University

CLOSED CIRCUIT TELEVISION (CCTV) POLICY

REVISED JULY 2015

ORIGINATOR(S)

Author(s)	Position
Alan Cain	Head of Security and Business Continuity
Ian Hamblett	Deputy Head of Security
Michelle Gretton	FOI and DPA Officer

APPROVED BY

Date	First Approval
08 July 2015	Health and Safety Committee

Date	Final Approval	
20 July 2015	Paul Kingsmore	Director of Services

SECTION 1 – INTRODUCTION

1.1 The University owns and operates a closed circuit television ("CCTV") scheme (the "CCTV Scheme").

1.2 The purpose of this policy is to:

1.2.1 outline the University's CCTV Scheme;

1.2.2 comply with the requirements of the Data Protection Act 1998, 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 Counter-Terrorism and Security Act 2015, and the University's Data Protection Policy;

1.2.3 set out the responsibilities of all employees (including temporary and contract staff) who are responsible for implementing, managing, operating or using the CCTV Scheme.

SECTION 2 – THE CCTV SCHEME

2.1 The CCTV Scheme comprises a number of cameras, installed at strategic locations. 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.

2.2 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' as defined in the Data Protection Act 1998 ("DPA 1998") and interpreted by the Courts.

2.3 The purposes of the CCTV Scheme are to:

2.3.1 help ensure a safer environment and reduce fear of crime;

2.3.2 facilitate the prevention and detection of crime, including the identification, apprehension and prosecution of offenders;

2.3.3 assist with the investigation of potential breaches of University regulations and/or actions which may result in disciplinary proceedings against students or staff;

2.3.4 assist the University with traffic management and car park access.

2.4 The Scheme 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 Services and the Legal Department.

2.5 The CCTV Scheme cannot prevent, cover or detect every incident which occurs within the University and/or the areas covered by the Scheme.

SECTION 3 – RESPONSIBILITIES

3.1 The University is responsible for the Scheme and is the registered data controller for the requirements of the Data Protection Act 1998.

3.2 The Head of Security & Business Continuity is responsible for the overall management and operation of the CCTV Scheme, including the training and licensing (where appropriate) of Security Guards / Public Space Surveillance CCTV Operators. No other CCTV installation or use by University employees is permitted without the authority of the Head of Security & Business Continuity.

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

3.3.1 only as authorised and in accordance with this Policy and the Data Protection Policy;

3.3.2 with respect for the privacy of individuals;

3.3.3 for the purposes described within this Policy and for no other purpose, unless required by law.

3.4 All CCTV operators are appropriately trained; and will be licensed if required by law.

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

SECTION 4 – IMPACT ASSESSMENT

4.1 The University carries out an assessment prior to installation of CCTV cameras, and reviews the Scheme periodically, to ensure adequate and appropriate use and compliance with the purposes for the CCTV Scheme as set out in section 2 of this policy and relevant legislation as set out in section 1 of this policy.

4.2 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.

4.3 Examples of considerations that the University may include in its assessments are: impact on crime; comparison of neighbouring areas without CCTV; consultation with relevant parties; the operation and effectiveness of this Policy; and a review of whether the purposes for the CCTV Scheme remain relevant.

SECTION 5 - SIGNAGE

5.1 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 signs at entrances to and within CCTV monitored zones. Signs are legible, visible, appropriately sized, relevant to the location, confirm that the University operates the CCTV; indicate the purposes of the Scheme; and who to contact regarding the Scheme.

5.2 Signs displaying an image of a camera state: "This CCTV Scheme is controlled by Manchester Metropolitan University. For further information contact the Security Control Room 0161 247 6656."

SECTION 6 – EQUIPMENT AND IMAGES

6.1 The CCTV Scheme's equipment 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:

6.1.1 CCTV equipment is checked, maintained and cleaned regularly to ensure it functions properly and clear images are recorded. Records of maintenance work are retained.

6.1.2 Where copies of recordings are required (e.g. for investigations / evidence) good quality CD-Rs/DVD-Rs are used (once only).

6.1.3 We have determined that it is necessary to record from every camera throughout the 24 hour period of every day, (subject to the camera working correctly).

6.2 CCTV images are not retained for longer than necessary for the purposes for which the images were recorded. The standard maximum retention period is 30 days, after which the images will be securely destroyed. Occasionally, images may be retained for longer to meet the purposes for which the images were taken, e.g., for investigating a crime or disciplinary matter.

6.3 CCTV images are kept securely in a controlled access area.

6.4 The CCTV Scheme does not routinely include areas requiring a heightened expectation of privacy (such as changing rooms or toilet areas).

6.5 All employees and workers responsible for managing, operating or otherwise using CCTV are trained in connection with this Policy.

SECTION 7 – ACCESS TO / DISCLOSURE OF IMAGES

7.1 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.

7.2 All requests for disclosure must be made in writing, including reasons / justification for the request and, where possible, relevant exemptions under the Data Protection Act / other legislation. All requests should be referred to the Head of Security & Business Continuity who will decide (in consultation with the Legal Department where appropriate / necessary) whether a disclosure can be made.

7.3 CCTV images may be released where the disclosure is necessary for the purposes for which the images were recorded (as set out in section 2 of this Policy) or where permitted / 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 (e.g. court order or information access rights).

7.4 A record of all requests for disclosure is retained, together with the reasons for disclosure or refusing the request. Where access / disclosure is approved, the following records are also retained (where relevant / applicable):

- Details / extent of information released;
- the date the images were copied / removed / released;
- person authorising the copy / disclosure;
- person making the copies / removal of images;
- details of recipients / person(s) viewing the images;
- signature of person collecting the images;
- crime incident number;
- current location of images;
- outcome of viewing;
- date / time images returned to Security.

7.5 Viewing of recorded images takes place in restricted areas and access is limited to authorised personnel during viewing.

SECTION 8 – SUBJECT ACCESS REQUESTS

8.1 Individuals whose images are recorded have a right to view the images of themselves and, if required, to be provided with a copy of the images. Requests must be made in writing to the Legal Department. The University is entitled to charge a fee of £10 for each subject access request received. The University aims to respond to requests within 40 calendar days. The person making the request must supply sufficient information to enable the University to identify him / her as the subject of the images, including the date / time / location, physical description and photograph. Data subjects are not entitled to receive images / personal data of any third party.

8.2 Where CCTV images reveal third parties (anyone other than the data subject), the images will be obscured so they are not recognisable.

8.3 For further information about information rights and the Data Protection Act see the University's Data Protection Policy at www.mmu.ac.uk/policy

SECTION 9 – CONTACTS AND COMPLAINTS

9.1 If you have any queries about this Policy, please contact the Head of Security and Business Continuity or the Legal Department.

9.2 We reserve the right to change this Policy from time to time to take into account any relevant changes in law or guidance from the Information Commissioner, or to reflect changes to the University's campuses.

9.3 Any complaint with regard to any aspect of the CCTV Scheme, will be investigated and dealt with in accordance with the guidance provided by the Information Commissioner's Office and any applicable policies and procedures of the University.