CCTV Policy

1. INTRODUCTION

1.1 Newman University has in place and is further developing a CCTV System "the System". Images are monitored and recorded centrally and will be used in strict accordance with this policy. The System is owned by Newman University, Genners Lane, Birmingham, B32 3NT.

1.2 The Estates and Facilities Manager is responsible for the operation of the System and for ensuring compliance with this policy, and compliance with any data protection legislation updates/changes in the future (in relation to CCTV).

2. THE SYSTEM

2.1.1 The System is made up of Fixed Positon Cameras, Pan Tilt and Zoom Cameras (PTZ), Automatic Number Plate Recognition Cameras and body-worn cameras.

2.1.2 Cameras are located at strategic points on the campus, principally at the entrance and exit points of the site and buildings. No camera will be hidden from view, and cameras will be prevented from focussing on private or neighbouring accommodation.

2.1.3 In accordance with national guidance and law, signs will be deployed advising staff, students, visitors and members of the public that a CCTV installation is in use.

2.1.4 Although every effort has been made to ensure the effectiveness of the System it is not possible to guarantee that the System will detect every incident taking place within the area of coverage.

2.1.5 This policy has no impact on recordings for use as part of the academic program, or the usage of cameras within lectures. Guidance can be obtained from the faculty offices/e-learning department if you have concerns about recordings of lectures.

2.2 Purpose of the System

2.2.1 The System has been installed by Newman with the primary purpose of reducing the threat of crime, protecting Newman's premises and helping to

ensure the safety of all Newman's staff, students and visitors consistent with respect for the individual's privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent.
- Assist in the prevention and detection of crime or civil offences.
- Facilitate the identification, apprehension and prosecution of offenders in relation to civil offences, crime and public order.
- Facilitate the identification of any activities/events which might warrant disciplinary proceedings being taken against staff or students.
- Assist in providing evidence to managers about staff or students against whom disciplinary or other action may be taken.
- Facilitate the movement of vehicles on site.
- In the case of security staff to provide management information relating to employee compliance with contracts of employment.

The System will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording and body worn cameras.
- For any automated decision making.

2.2.2 The University seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy.

2.3 Covert recording

2.3.1 Covert cameras may be used under the following circumstances:

a) When informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; **and**

b) When there is reasonable cause to suspect that activity which is unauthorised by the University or illegal is taking place or is about to take place; **and**

c) When it has been authorised. The Vice-Chancellor (or University Leadership Team nominee) is empowered to authorise covert recording. If someone wishes to request covert recording they need to contact an appropriate member of staff, (normally a member of UOT or the Facilities Manager), who will review and consider requesting authorisation. In cases where the Vice-Chancellor is a subject of covert recording the Clerk to the University Council will be empowered to make the authorisation. Where both the Vice-Chancellor and Clerk to the University Council are the subjects of covert recording, another member of ULT with a member of

the University Council (with the exception of the staff or student members of Council) would be required to authorise the covert recording.

2.3.2 Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorised activity.

2.3.3 The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

2.3.4 The Covert Recording Policy must be consulted before authorisation is granted and before covert recording is carried out.

2.3 Body-Worn Cameras

2.4.1 Body-worn cameras may be used during security/hall tutors' patrols and incident attendance. The body-worn camera will display a green light to inform users they are being recorded. As they approach an incident, staff should also disclose to people that they are being visually and audio recorded.

2.4.2 The downloading of images from such cameras will only be conducted by trained staff, and cameras will be cleansed following each shift. Downloading will be conducted on the PCs in the Security and Porters area. These images should only be retained for the duration of any case/appeal, and sufficient time for an external review. After this time they should be securely destroyed. For criminal cases, these recordings will be handed over to the Police or other crime agency. All other recordings will be deleted immediately after review.

3 PRIVACY IMPACT ASSESSMENTS AND DATA PROTECTION

3.1 The Surveillance Camera Commissioner's Code of Practice states the need for Privacy Impact Assessments and provides templates for these assessments. It is noted that the Privacy Impact Assessment template provided by the Surveillance Camera Commissioner is dated from before the new legislation but is more specific in assessing risk than that provided by the ICO. Therefore the University will follow this Code of Practice and use the provided templates in their current form and will update terminology when the Code of Practice is updated in the light of current data protection legislation.

3.2 Privacy Impact Assessments will be carried out for all CCTV installations on campus.

3.3 Privacy Impact Assessments will be retained by the Estates and Facilities Manager.

3.4 Privacy Impact Assessments should be reviewed annually to consider the necessity and location of the cameras.

3.5 The University will use the Surveillance Camera Commissioner's Guidance forms to conduct the Privacy Impact Assessments.

3.6 As required by the ICO and Surveillance Camera Commissioner, signs will be displayed at all entrances to the University Campus.

3.7 In its administration of the System, the University complies with current data protection legislation.

The privacy principles in Article 5(1) requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, Article 5(1) ('accountability')."

3.8 The lawful basis for processing the personal data within the System is legitimate interests.

4. THE SECURITY CONTROL ROOM

4.1 Images captured by the system will be monitored and recorded in the Security Control Room, "the Control Room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room. Please refer to operation manual for the Control Room.

4.2 No unauthorised access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorised members of senior management, police officers and any other person with statutory powers of entry.

4.3 Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorisation from the Estate and Facilities Manager. This request must be written or emailed to the Estates and Facilities Manager. Where a decision has been declined this can be appealed using the University complaints procedures. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter the Control Room.

4.4 A person accessing the Control Room must surrender their phone and other devices capable of taking photos or video. These devices will be surrendered to the security guard on duty, and returned to the person when they leave the Control Room.

4.5 Before allowing access to the Control Room, staff must satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. All visitors, including those granted emergency access, are required to complete and sign the visitors' log, which includes details of their name, their department or organisation they represent, the person who granted authorisation, the reason for entry and the times of entry to and exit from the Control Room. A similar log is kept of the staff on duty in the Control Room. The sign in logs, which contain personal data, will be kept for one year. After this period the data will be anonymised and kept indefinitely for statistical purposes. Sign in logs will be available to the security staff and the Estates and Facilities Management Team.

4.6 Footage will be stored securely, for example, encrypted or in locked storage. Access is tracked by a signing process. Security measures are in place to ensure that CCTV footage is not tampered with.

4.7 In addition to this policy, please refer to the operation manual for staff using the Control Room. This is a joint document between the security operator and the University.

5 REQUESTS FOR DISCLOSURE OF IMAGES

5.1 Requests from data subjects

5.1.1 A request by a data subject for images relating to themselves is called a Data Subject Access Request (DSAR). Requests should be made after reading the information on the University DSAR webpage where a DSAR form is available. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of their personal data, subject to exemptions contained in the law. However, they do not have the right of instant access.

5.1.2 The Data Protection Officer will then review the DSAR and, subject to lawful exemptions, arrange for a copy of the data to be made and given to the requester. The requester must not ask another member of staff to show them the data, or ask anyone else for a copy of the data. All communications must go through the Data Protection Officer. A response will be provided without undue delay and at the latest within one month of receipt of the DSAR.

5.1.3 In order to locate the images on the University's system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.

5.1.4 Where the University is unable to comply with a DSAR without disclosing the personal data of another individual who is identifiable from that information, it is not obliged to comply with the request unless satisfied that the other individual has provided their express consent. Where it is unreasonable or impractical to request or receive such consent the Data Protection Officer will advise the University on whether to disclose the personal data.

5.1.5 The law gives the University the right to refuse a request for a copy of the personal data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. The Data Protection Officer will advise the University on this matter.

5.1.6 If the University decides not provide a copy of the personal data requested, the reasons will be documented and the requester will be informed in writing.

5.2 Access by third parties or the University

5.2.1 A request for images made by a third party should be made in writing to the Estates and Facilities Manager, who must inform the Data Protection Officer of the request.

5.2.2 In limited circumstances it may be appropriate to disclose images to a third party, such as when a disclosure is required by law in relation to the prevention or detection of civil offence or crime, or in other circumstances where an exemption applies under relevant legislation.

5.2.3 Such disclosures will be made at the discretion of the Estates and Facilities Manager, with reference to relevant legislation and where necessary, following advice from the University Secretary and Registrar, Director of HR, or Data Protection Officer.

5.2.4 Where a suspicion of staff misconduct arises and at the formal request of the Director of HR/HR Manager, the Estates and Facilities Manager may provide access to CCTV images for use in staff disciplinary and grievance cases.

5.2.5 The Estates and Facilities Manger may provide access to CCTV images to Investigating Officers when sought as evidence in relation to student disciplinary cases. If concerns are held about the images being supplied, advice may be obtained from the University Secretary and Registrar before images are provided to the Investigating Officer.

5.3 **Record of Disclosure**

5.3 A record of any disclosure made under this policy will be held on the CCTV Camera Access log, itemising the date, time, camera, requestor, authoriser, eprocessor and reason for the disclosure. This log, which contains personal data, will be kept for one year. After this period the data will be anonymised and kept indefinitely for statistical purposes.

6. RETENTION OF IMAGES

6.1 Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 45 days from the date of recording. Images will be automatically overwritten after this point.

6.2 Where an image is required to be held in excess of the retention period referred to in 6.1, the Estates and Facilities Manager or their nominated deputy, will be responsible for authorising such a request. This will be noted in the CCTV Register.

6.3 Images held in excess of their retention period will be reviewed on a three-monthly basis and any not required for evidential purposes will be deleted.

6.4 Access to retained CCTV images is restricted to the Estates and Facilities Manager and other persons as required and as authorised by the Estates and Facilities Manager. This will be recorded in the CCTV Camera Access Log.

6.5 Images and recordings that have been supplied for evidential purposes, the investigation of an offence or as required by law, should be deleted a reasonable time after the case is closed or dismissed. When determining the definition of a 'reasonable time', consideration should be given to whether there is likely to be an appeal or escalation to an external agency. A note

should be added to the case file explaining why the footage has been kept. For certain appeals, this could take 15 months from the date of the closure letter. Guidance should be sought from the University Secretary and Registrar if the personal data is to be retained for a longer period.

7. COMPLAINTS PROCEDURE

7.1 Complaints about the System or about the disclosure of CCTV images should be made, in the first instance, to the Estates and Facilities Manager (estates@newman.ac.uk). This is in accordance with the Informal Stage of the University's complaints procedures.

7.2 All appeals against a decision of the Estates and Facilities Manager should be made using the University's complaints procedures.

Members of the Public Complaints Procedure
Student Complaints Procedure
Staff Grievance Procedure

8. MONITORING COMPLIANCE

8.1 All staff involved in the operation of the System will be made aware of this policy and will only be authorised to use the System in accordance with this policy.

8.2 All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake data protection training.

8.3 Security Staff and University Security Managers will undertake appropriate Security Industry Authority (SIA) training, and will be licenced with the SIA.

8.4 This policy will be available to view at all times in the Control Room, for operators to refer to. A copy of this policy will be available in the Control Room for anyone to view by request at any time. It is also available on the University website.

9. POLICY REVIEW

9.1 The University's usage of CCTV and the content of this policy shall be reviewed every two years by the Facilities Manager with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.