CCTV CODE OF PRACTICE

Policy area: Operation of CCTV on University Premises

Definitions

"CCTV" means Closed Circuit Television.

"Control Room(s)" means those Control Rooms manned by Security staff at the City, Clifton or Brackenhurst Campuses.

"Data Subjects" means an individual who is a subject of personal data.

"NTU and the **"University"** both mean Nottingham Trent University.

"Security Manager" shall mean, for the purposes of this policy, the member of staff with specific responsibility for management and control of the University's CCTV systems or his/her nominee.

"System" means the University's CCTV Surveillance System including CCTV cameras.

Contents

1. Introduction

1.1 The University has installed a comprehensive CCTV surveillance system across all three campuses for the principal purposes of preventing and detecting crime. The images from the CCTV system can be monitored in the control rooms at each campus, which are staffed by the University's Security Department. It is recognised that ancillary benefits of operating CCTV for this purpose may include reduction of the fear of crime generally and the provision of a safer public environment for the benefit of those who live or work within and visit the University.

1.2 CCTV Cameras which are located within individual buildings are capable of being monitored by the Reception Officers of those buildings. If the Security Manager considers that the security of a College/School or Professional Services Department whose areas the cameras are designed to protect would be improved by allowing designated staff within that area to monitor the images, then relevant staff will be authorised to view the images. CCTV images monitored by Reception Officers will show live images only and will not include external cameras or give access to archived images

1.3 The University's CCTV surveillance system has been installed and is monitored in line with the following objectives:

- 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 aid public safety; and
- To assist with the management of the University's car parks.
- To assist Student and Staff Support Services in connection with disciplinary procedures in cases of serious misconduct; and
- To assist in room utilisation surveys.

1.4 Due to public concern surrounding a surveillance society, the use of CCTV surveillance must be consistent with respect for individuals' privacy and due to this concern other methods of achieving the objectives of a CCTV surveillance system will be considered before installation of any CCTV camera on the University campuses.

1.5 This Code of Practice has been prepared for the guidance of University staff and students. Its purpose is to ensure that the CCTV system is used to create a safer environment for staff, students and visitors to the University and to ensure that its operation is consistent with the obligations on the University imposed by the Data Protection Act 1998, Article 8 of the Human Rights 1998 and The Security Industry Authority. For the purposes of the Data Protection Act 1998, the Data Controller is Nottingham Trent University.

2. Operation of the University's CCTV Surveillance System

<u>The System</u>

2.1 The system is operational and images are capable of being monitored for twenty-four hours a day throughout the whole year.

2.2 The public and University community are made aware of the presence of the system by appropriate signage which sets out the purposes for processing the CCTV images and identifies the University as the party responsible for processing those images.

2.3 To ensure privacy, wherever practicable, the CCTV cameras are prevented from focusing or dwelling on domestic accommodation. Where domestic areas such as gardens abut those areas which are intended to be covered by the scheme, the Security Manager 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 abut the areas which are intended to covered, appropriate training will be given to system operators to ensure that they are made aware that they should not be monitoring such areas.

2.4 Images captured by cameras will be recorded on equipment located securely within University buildings. All security control rooms will have monitoring equipment which will allow control room officers to monitor live images from the cameras, any transfer of images onto other media will only take place within the City Control room in line with this Code of Practice.

2.5 Although every reasonable effort has been made in the planning and design of the CCTV system to give it maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the areas of coverage.

Control Rooms

2.6 Images captured by the system will be monitored in the self-contained and secure Control Rooms. CCTV cameras monitored by Reception Officers show live images only.

2.7 Access to Control Rooms is strictly limited to the Duty Controllers, authorised staff members and Senior Management. Police Officers may enter with the explicit consent of the Security Manager. Other persons may be authorised to enter the Control Room on a case-by-case basis with the explicit consent of the Security Manager with each visit being supervised at all times.

2.8 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. Before access is granted to any person, the Security Manager must be satisfied with the identity of any visitor.

2.9 All visitors will be required to complete and sign a visitors' log which will be kept in the Control Room.

2.10 An incident log will be maintained in the Control Room with full details of security incidents including those captured on CCTV which are transferred to another medium, together with any consequential action taken.

2.11 Handling of images and information within the Control Rooms will be done in accordance with this Code of Practice and the Data Protection Act 1998. The Security Manager will be responsible for compliance with section 2.2.5 above and for the development of working procedures within the control room to ensure such compliance.

3. Monitoring of CCTV Images

3.1 The Security Manager will ensure that all staff (including relief/temporary staff) are fully briefed and trained in respect to all functions, both operational and administrative, arising within the operation of CCTV surveillance including training in the requirements of this Code of Practice and the Data Protection Act 1998.

3.2 The control of the CCTV Surveillance System will always remain with the University. However, at the Security Manager's discretion, the cameras may be operated in accordance with requests made by the police during an incident to monitor potential public disorder, assist in the detection of crime or facilitate the apprehension and prosecution of offenders in relation to crime and public order. On each occasion the Police are assisted with their operations, a report setting out the time, date and detail of the incident will be submitted to the Security Manager.

3.3 CCTV images which evidence any behaviour, which cannot reasonably be ignored, may be used for staff and student disciplinary purposes.

Covert Monitoring

3.4 Covert monitoring will only be considered in exceptional circumstances. Deployment will be subject to the completion of an impact assessment[1], in line with Part 3 of the ICO's Data Protection, Employment Practices Code and approval by both the Security Manager and the Director of Human Resources or PVC for Student Affairs, in the case of students.

3.5 Circumstances where covert monitoring may be considered include; where there are grounds for suspecting criminal activity or equivalent malpractice, where notifying the individuals about the monitoring would prejudice its prevention or detection.

3.6 Where covert monitoring is approved, it must be strictly targeted at obtaining evidence within a set timeframe and must cease once the investigation is complete.

3.7 Images recorded of individuals not under suspicion will be deleted.

4. Recording of Images and Access

Control and Management of Recordings

4.1 All recording media used for the monitoring and capture of images on the University's CCTV system belongs to and remains the property of the University.

4.2 The Control Rooms are supported by a digital recording system which stores images on appropriate media until capacity is reached and the images are then automatically overwritten.

4.3 Should it be decided that images be retained for any reason, including for release to a third party (including the Police) under the exemptions contained within sections 28(1), 29(1)(a) and (b) and/or 35(2)(a) of the Data Protection Act 1998, or retained for any reason for which the system is registered with the Information Commissioner, copies of those images may be transferred to an appropriate computer file.

4.4 Any file stored in line with 4.1.3 above shall be given a unique reference number by the person creating the file and a record made in an image tracking register contained within the control room.

4.5 Unless required for any of the reasons contained within Section 29(3) of the Data protection Act 1968, recorded images will be retained for no longer than required for the purpose for which they were originally obtained, after that time the images are automatically overwritten by the recording equipment

4.6 Any recording medium will be cleaned before re-use to ensure that images are not recorded on top of images previously recorded.

---

[1] The impact assessment should be completed by the manager appointed to investigate the alleged misconduct.

Access to Recordings by Staff or Third Parties

4.7 It is important that access to and disclosure of images is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. These aspects of the Code of Practice reflect the Second and Seventh Data Protection Principles of the Data Protection Act 1998.

4.8 Access to recorded images will be restricted to security staff and those staff who require access, following the consent of the Security Manager, in order to achieve the purposes of using the equipment.

4.9 Requests by persons outside the University (other than the Police) for viewing or obtaining recordings will be assessed on a case by case basis by the Security Manager and access will only be granted where it is consistent with the obligations placed on the University by the Data Protection Act 1998.

4.10 All requests for access will be recorded detailing the date and time at which access was allowed/or disclosure made; the reason for the access/disclosure; the extent of the information accessed/disclosed; name of the security staff providing access.

4.11 If access to images is denied to any member of staff or third party (including the Police), the Security Manager will document the reasons for the denial and the information will be logged at the Control Room.

4.12 Where it is decided by the Security Manager that the assistance of a member of University staff is needed to identify a victim, witness or perpetrator in relation to a criminal incident, images from the system may be circulated via the University's email system to selected staff on a targeted basis, or placed on a suitably restricted area of the University's website. As part of that decision, the wishes of the victim of an incident will, where possible, be taken into account.

Access by the Police

4.13 Where a police officer requests access to CCTV images either by viewing such data or requesting a copy of the data, the requisite form (held by Security) must be completed and signed.

4.14 Requests for access to images by the Police will not normally be denied and can be made without the authority of the Security Manager provided they are accompanied by a written request signed by a Police Officer, who must indicate that the images are required for the purposes of a specific crime enquiry.

Access by Data Subjects

4.15 The University will comply with section 7 of the Data Protection Act 1998 in informing individuals whether or not information relating to them (in this case images) have been processed by the CCTV Surveillance System. The University is not obliged to comply with a request under this section unless it is supplied with such information as it may reasonably require to satisfy itself as to the identify of the person making the request and to locate the information which that person seeks.

4.16 Data Subjects may make a subject access request for CCTV images/recordings/information (request for data about themselves) by using the required form which is available from http://www.ntu.ac.uk/freedom_of_information_act/requesting_information/15351gp.html and must provide the following information:

Dates and times of the incident or their visit to the University with details of the location on the NTU campus;
two photographs –one full face and one side view;
proof of identity (e.g. driving licence/passport containing a photograph); Cheque or cash in the sum of £10.00;
Whether they require copies or view of the images in question.

4.17 A written decision will be sent to the data subject within 21 days of receipt of the request. If access is agreed, such access will be provided within 40 days of receipt of the request or, if later, on the date when the University receives confirmation of identification from the data subject.

4.18 Where the University is unable to comply with a subject access request without disclosing information relating to another individual who can be identified from that information, it is not obliged to comply with the request unless that individual has consented to the disclosure or it is reasonable, in the circumstances, to comply without the consent of the individual.

5. Complaints

5.1 Breaches of this Code by Security, Reception and other staff monitoring the system or who have access to the monitored images may constitute matters of discipline under the relevant conditions of employment.

5.2 It is also recognised that other members of the University may have concerns or complaints in respect to the operation of the CCTV Surveillance System. Any concerns or complaints should, in the first instance, be addressed to the Security Manager.

5.3 Concerns or queries relating to the Data Protection Principles in general should be directed to Legal Services.

6. Other Supporting Documents

Corporate Guidelines on Data Protection.

Enrolment Conditions – for use of student data.

7. Governance

Responsibility

Policy Owner	The Security & Operations Manager

Version Control and Change History

Version Number	Approval Date	Approved by	Amendment
1.0	January 2009		New Policy
1.1	December 2009		Annual Review
2.0	June 2011		Revised Version
3.0	December 2017		Revised Version

Document Review

The Policy and Procedure will be reviewed by the Security & Operations Manager in association with Legal Services, the trade unions, employee representatives (where appropriate) and managers in response to statutory changes, changes in University procedures or structures or as a result of the monitoring of the application of the procedure. In any event, the Policy and Procedure will be reviewed every two years.