Nottingham University Academy of Science and Technology

CCTV Code of Practice

Responsible officer: Principal

Date approved: 21/11/2016

Review date: November 2018

Approved by: NUAST Board of Directors

NOTTINGHAM UNIVERSITY ACADEMY OF SCIENCE AND TECHNOLOGY

CCTV System Code of Practice
(Part of the Data Protection Policy)

1. Introduction

1.1 The purpose of this code of practice is to regulate the management, operation and use of the closed circuit television (CCTV) system at the Nottingham University Academy of Science and Technology (the Academy).

1.2 The system comprises fixed and dome cameras located around the Academy's site(s). All cameras are monitored within the Academy and by any preferred monitoring companies it may engage.

1.3 This Code follows Data Protection Act guidelines.

1.4 The Code of Practice will be subject to review periodically, but at least biennially, to include consultation as appropriate with interested parties.

1.5 The CCTV system is owned by the Academy.

2. Objectives of the CCTV System

a. To protect the Academy's buildings and its assets
b. To increase personal safety and reduce the fear of crime
c. To support the Police in a bid to deter and detect crime
d. To assist in identifying, apprehending and prosecuting offenders
e. To protect members of the public and private property
f. To assist in managing the Academy.

3. Statement of intent

3.1 The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

3.2 The Academy will treat the system and all information, documents and recordings obtained and used as data which is protected by the Act.

3.3 Cameras will be used to monitor activities within the Academy and its car parks and other public areas to identify criminal activity actually occurring, anticipated or perceived, and for the purpose of securing the safety and well being of the Academy, together with its visitors.

3.4 Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.

3.5 Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained using the Academy's forms for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

3.5 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Digital information will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police. Digital information will never be released to the media for purposes of entertainment.

3.6 The planning and design of the CCTV system has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3.7 Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the Academy's CCTV.

4. Operation of the system

4.1 The Scheme, as part of the overall Data Protection Policy, will be the responsibility of the Principal or designate, in accordance with the principles and objectives expressed in the code.

4.2 The day-to-day management will be the responsibility of the Estates Manager or designate during the day.

4.3 The CCTV system will be operated 24 hours each day, every day of the year.

4.4 The Site Manager will confirm the efficiency of the system on a periodic basis and in particular that the equipment is properly recording and that cameras are functional.

5. Physical access to the system

5.1 Access to the CCTV facilities will be strictly limited to members of the Senior Leadership Team, Site/Security Officer(s) and Estates Manager. All hardware is held within a secure room, providing additional access barriers.

5.2 Unless an immediate response to events is required, the above staff must not direct cameras at an individual or a specific group of individuals.

5.3 Approved contractors only should be used for maintenance, specifically out of hours. All such visits should be logged including the time of entry and exit.

5.4 Other administrative functions will include maintaining digital images on the hard disc space, filing and maintaining occurrence and system maintenance logs.

6. Liaison

Liaison meetings may be held with all bodies involved in the support of the system.

7. Monitoring procedures

7.1 Camera surveillance may be maintained at all times.

7.2 A secure facility is available to the Estate Manager and relevant other staff listed in Section 5, to which pictures will be continuously available.

7.3 If covert surveillance is planned or has taken place copies of the Authorisation Forms, including any Review must be completed and retained.

8. Recorded media procedures

8.1 In accordance with published guidance, data stored on the dedicated disks is retained for the minimum period consistent with our needs for recording the data. This retention period is 30 days, at which point the disks are automatically overwritten.

8.2 Digital evidence may be viewed by the Police for the prevention and detection of crime.

8.3 A record will be maintained of the release of digital information to the Police or other authorised applicants. A register will be available for this purpose.

8.4 Viewing of digital evidence by the Police (appropriately authorised) must be recorded in writing and in the log book.

8.5 Digital evidence will only be released to the Police on the clear understanding that the digital evidence remains the property of the Academy, and the digital evidence to be treated in accordance with this Code. The Academy also retains the right to refuse permission for the Police to pass to any other person the digital evidence.

8.6 The Police may require the Academy to retain the digital evidence for possible use as evidence in the future. Such digital evidence will be properly indexed and securely stored until it is needed by the Police.

8.7 Applications received from outside bodies (e.g. solicitors) to view or release digital evidence will be referred to the Principal. In these circumstances digital evidence will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

9. Breaches of the Code (including breaches of security)

9.1 Breaches of the Code and remedies will be reported to the Principal.

9.2 Any breach of the Code of Practice by Academy staff will be investigated in accordance with the disciplinary procedures.

9.3 Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

10. Assessment of the scheme and Code of Practice

Performance monitoring, including random operating checks, may be carried out by the Principal or designate.

11. Complaints

11.1 Any complaints about the Academy's CCTV system should be addressed to the Estates Manager in the first instance.

11.2 Complaints will be investigated initially by the Estates Manager and escalated if appropriate.

12. Access by the data subject

12.1 The Data Protection Act provides Data Subjects (individuals to whom "personal data" relates) with a right to data held about themselves, including those obtained by CCTV.

12.2 Requests for Data Subject Access should be made in writing to the Estates Manager.

13. Public information

13.1 Copies of this Code of Practice will be available to the public from the Principal.

13.2 Summary of Key Points

a. This Code of Practice will be reviewed every two years
b. The CCTV system is owned and operated by the Academy
c. The Control system is not accessible to visitors except by prior arrangement and with good reason
d. Liaison meetings may be held with the Police and other bodies
e. All recording media will be used properly, indexed, stored and destroyed after appropriate use
f. Digital information may only be viewed by authorised Academy Officers and the Police
g. Digital information required as evidence will be properly recorded, witnessed and packaged before copies are released to the Police
h. Digital information will not be made available to the media for commercial or entertainment purposes
i. Digital information will be disposed of securely
j. Any breaches of this Code will be investigated in accordance with the Academy's disciplinary procedures. An independent investigation will be carried out for serious breaches
k. Breaches of the Code and remedies will be reported to the Principal.