CCTV POLICY

1. INTRODUCTION

1.1. The purpose of this policy is to regulate the management and use of the closed circuit television (CCTV) system at Fundamental Movement Academy.

1.2. The system comprises of a main control unit and a number of fixed cameras located around the Academy site. All cameras are monitored from within the Academy. The main control unit is held in a secure location.

1.3. This CCTV scheme and policy is operated within the Information Commissioner's Code of Practice for CCTV 2008 and Surveillance Camera Code of Practice 2013 published by the Home Office.

1.4. This policy will be subject to annual review, which will include a review in respect of the effectiveness and necessity of the system.

1.5. The CCTV system is a digital system which is owned wholly by the Academy. The system does not make audio recordings.

2. OBJECTIVES OF THE CCTV SCHEME - Along with a range of measures, the CCTV system will be used to:

2.1. Help maintain an environment for students, staff and others, which supports their safety and welfare.

2.2. Deter crime against persons, and against the Academy buildings and Academy assets.

2.3. Assist in the identification and prosecution of persons having committed an offence.

2.4. Record accidents.

2.5. Act as a viewing stream for spectators.

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, as well as the Surveillance Camera Code of Practice 2013 published by the Home Office.

3.2. The Academy will treat as data all CCTV recordings and relevant information.

3.3. Cameras will be used to monitor activities within the Academy in line with the objectives of the scheme.

3.4. 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 in writing for directed surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

Contd.

3.5. Materials or knowledge secured as a result of CCTV will not be released to the media, or used for any commercial purpose, or for the purpose of entertainment. Recordings will only be released under the written authority from the Police, or in respect of a subject access request 2.4 and 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 Academies CCTV.

4. OPERATION OF THE SYSTEM

4.1. The system will be administered by the Manager and Committee and relevant premises staff, in accordance with the principles and objectives expressed in the code.

4.2. The CCTV system will be in operation 24 hours each day, for every day of the year.

4.3. The Manager will check on a weekly basis that the system is operating effectively in particular that the equipment is properly recording and that cameras are functional. The system will be regularly serviced and maintained. Defects will be reported to the servicing company at the earliest convenient opportunity.

5. CONTROL OF SOFTWARE & ACCESS TO THE SYSTEM

5.1. Access to the CCTV software will be strictly limited to authorised personal only.

5.2. Unless in an immediate response to events, staff using the CCTV software must not direct cameras at an individual or a specific group.

5.3. Operators must satisfy themselves that all persons viewing CCTV material will have a right to do so.

5.4. The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption.

5.5. The main control facility must be kept secure.

5.6. Other administrative functions will include controlling and maintaining downloaded digital materials, and maintenance and system access logs.

6. MONITORING PROCEDURES

6.1. Camera surveillance will be maintained at all times.

6.2. A monitor is installed in the main control room. Access to monitors must be restricted to staff where those areas being monitored are not in plain view.

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

7. DIGITAL IMAGES: PROCEDURES

7.1. Live and recorded materials may be viewed by authorised operators in investigating an incident, accident and recorded material may be downloaded from the system in line with the objectives of the scheme.

Contd.

7.2. Images (stills and footage) may be viewed by the Police for the detection of crime.

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

7.4. Viewing of images by the Police must be recorded in writing. Requests by the Police are allowable under section 29 of the Data Protection Act (DPA) 1998

7.5. Should images be required as evidence, a digital copy may be released to the Police. The Academy retains the right to refuse permission for the Police to pass the images to any other person.

7.6. The Police may require the Academy to retain images for possible use as evidence in the future. Such images will be securely stored until they are needed by the Police .

7.7. Applications received from outside bodies (e.g. solicitors) to view or release images will be referred to the Manager. In these circumstances, images 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 may be charged of £10 in such circumstances, which is appropriate for subject access requests.

7.8. Retention: Images will be retained for only as long as these are required. The system will automatically delete all recordings held on the main control unit after approximately one month.

8. BREACHES OF THE CODE (including breaches of security)

8.1. Any breach of the CCTV Code of Practice by Academy staff will be investigated by the Manager.

9. ASSESSMENT OF THE SCHEME AND CODE OF PRACTICE

9.1. Performance monitoring, including random operating checks, may be carried out by the Manager

10. COMPLAINTS

10.1. Any complaints about the Academies CCTV system should be addressed to the Manager.

11. SUBJECT ACCESS AND FREEDOM OF INFORMATION

11.1. 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 11.2. Requests for Data Subject Access should be made in writing to the Manager.

11.3. A request for Subject Access will be charged at £10, which is the maximum allowable under the Data Protection Act.

11.4. A request under the Freedom of Information Act 2000 will be accepted, when such a request is appropriate copies of this policy and CCTV Code of Practice (below) will be available on the Academies website.

APPROVED JUNE 2020