Sedgehill Academy
The best in everyone
Part of United Learning

CCTV POLICY

Approved by Governing Body: October 2023
For Review: October 2024
Date: October 2023

Sedgehill Academy
London, SE6 3QN

Prepared by: Samuel Harry (Cluster Facilities Manager)

Contents

1. Introduction

1.1 Sedgehill Academy has in place a CCTV surveillance system "the CCTV system" across its premises. This policy details the purpose, use and management of the CCTV system in the Academy and details the procedures to be followed in order to ensure that the Academy complies with relevant legislation and the current Information Commissioner's Office Code of Practice.

1.2 The Academy will conform to the requirements of the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and any subsequent data protection legislation, and to the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. Although not a relevant authority, the Academy will also have due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and in particular the 12 guiding principles contained therein.

1.3 This policy is based upon guidance issued by the Information Commissioner's Office, 'In the picture: A data protection code of practice for surveillance cameras and personal information' ("the Information Commissioner's Guidance").

Introduction | ICO

2. CCTV System overview

2.1 The CCTV system is owned by Sedgehill Academy (in conjunction with Kier) and managed by the Academy and its appointed agents. The data controller for CCTV images held by Sedgehill Academy is United Learning Trust (ULT). ULT is registered with the Information Commissioner's Office (ICO). The registration number is Z7415170.

The Group's Data Protection Officer, Alison Hussein, is responsible for ensuring that ULT complies with the Data Protection Law. She can be contacted on company.secretary@unitedlearning.org.uk or 01832 864538

The CCTV system operates to meet the requirements of the Data Protection Act 2018 and the Information Commissioner's Guidance.

2.2 Sedgehill Academy's Cluster Facilities Manager is responsible for the overall management and operation of the CCTV system, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

2.3 The CCTV system operates across the Academy. Details of the number of cameras can be given on request.

2.4 Clearly visible signs are placed at all pedestrian and vehicular entrances to inform staff, pupils, parents, visitors and members of the public that CCTV is in operation. The signage indicates that the system is managed by the Academy.

2.5 The Data Protection Lead is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.

2.6 Cameras are sited to ensure that they cover Academy premises as far as is possible. Cameras are installed throughout the Academy's sites including roadways, car parks, buildings (internal and external), within buildings and externally in vulnerable public facing areas.

2.7 Cameras are not sited to focus on private residential areas. Where cameras overlook residential areas, privacy screening or software masking will be utilised.

2.8 The CCTV system is operational and capable of being monitored for 24 hours a day, every day of the year.

2.9 Any CCTV installation shall be subject to a Data Protection Impact Assessment. It will also comply with the policy and procedures within this document. The Data Protection Impact Assessment shall be appended to this policy and shared with Central Office Data Protection Officer

3. Purposes of the CCTV system

3.1 The principal purposes of the Academy's CCTV system are as follows:
- for the prevention, reduction, detection and investigation of crime and other incidents;
- to ensure the safety of staff, children, visitors and members of the public; and
- to assist in the investigation of suspected breaches of Academy regulations by staff or students.

3.2 The CCTV system will be used to observe the Academy's buildings and areas under surveillance to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.

3.3 The Academy seeks to operate its CCTV system in a manner that is consistent with respect for the individual's privacy as outlined in the Privacy Impact Assessment.

4. Monitoring and Recording

4.1 Cameras are monitored in reception and reception office within the main building.

4.2 Images are recorded centrally on servers located securely in the Server Room located in the Kier site office and are viewable in the reception office by all CCTV trained staff. CCTV can also be viewed within the Kier site office. Additional staff may be authorised by the Principal to monitor cameras on a view only basis to support trained staff i.e. in identifying specific children.

Trained staff are as follows: Assistant Principals, Head of Sixth Form, Principal, Office Manager, Vice Principal, Cluster Facilities Manager, Facilities Manager – Kier, Senior Network IT Technician

4.3 A log shall be kept of requests to access recorded images by staff and whether any recorded images have been copied to support specific investigations. Information logged will include Name of staff, time and date of viewing, time and date of images reviewed, brief reason for viewing content (e.g. "incident in corridor") but will not contain names, whether any images have been copied and where they have been copied to.

4.4 The cameras installed will provide images that are of suitable quality for the specified purposes for which they are installed, and all cameras are checked regularly to ensure that the images remain fit for purpose and that the date and time stamp recorded on the images is accurate.

4.5 All images recorded by the CCTV System remain the property and copyright of United Learning. The recorded images are stored onsite on a server. Downloaded footage used in investigations is securely stored onsite on a server, in accordance with the process outlined in the retention of images section.

4.6 The CCTV system will not be used to carry out lesson observations.

4.7 The use of cameras in areas where one would normally expect a degree of privacy should be clearly identified on the Privacy Impact Assessment. This would include cameras placed in, or looking into, toilet or changing areas.
Cameras are only be used in toilet or changing areas where there are full height cubicles, never in areas where it is possible to see people using the toileting facilities (excluding hand washing) or changing.

4.8 The use of covert cameras is restricted to rare occasions, when a series of criminal acts have taken place within a particular area that is not otherwise fitted with CCTV. A request for the use of covert cameras will clearly state the purpose and reasons for use and the authority of both the Principal and Director of People will be sought before the installation of any covert cameras. The Principal should be satisfied and be able to demonstrate that all other physical methods of prevention have been exhausted prior to the use of covert recording.

4.9 Covert recording will only take place if informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there are reasonable grounds to suspect that illegal or unauthorised activity is taking place. All such monitoring will be fully documented and will only take place for a limited and reasonable period.

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

5. Compliance with Data Protection Legislation

5.1 From 25 May 2018, the Academy comply with the General Data Protection Regulation. Due regard is given to the data protection principles contained within Article 5 of the GDPR which provide that personal data is:

a. processed lawfully, fairly and in a transparent manner;

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date;

e. kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2 All storage used for images, recorded or downloaded for investigations, will be in compliance with GDPR rules; on secure storage on premise or on cloud storage within the EEA

5.3 The existence of the Academy's CCTV system must be recorded in the Record of Data Processing Activities using United Learning's Education Information Portal (EIP).

6. Applications for disclosure of images

Applications by individual data subjects

6.1 Requests by individual data subjects for images relating to themselves "Subject Access Request" must be submitted in writing.

6.2 In order to locate the images on the Academy'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.

6.3 Where the Academy is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual. Any decision to withhold the requested images must be referred to the Group's Data Protection Officer or his team as there are specific rules that must be adhered to when applying the exemptions contained in the Data Protection Act 2018.

Access to and disclosure of images to third parties

6.4 A request for images made by a third party must be made in writing.

6.5 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 crime or in other circumstances where an exemption applies under relevant legislation.

6.6 All unexpected requests for CCTV images by a third parties, including requests made by the police, should be referred to the Academy's Data Protection Lead in the first instance and if not available to the Group's Data Protection Officer or their team, who will advise on the application of any appropriate exemptions. Any third-party request should be added to the EIP in the GDPR area under *third party request*s.

6.7 Where a suspicion of misconduct arises and at the formal request of the Investigating Officer or HR Manager/ Business Partner, the Principal may provide access to CCTV images for use in staff disciplinary cases.

6.8 The Principal may provide access to CCTV images to Investigating Officers when sought as evidence in relation to staff discipline cases.

6.9 A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

7. Retention of images

7.1 Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 30 days from the date of recording. Images will be automatically overwritten after this point.

7.2 The automatic deletion of data after the defined retention period is checked on a half termly basis. This should be logged on a half termly basis.

7.3 Where an image is required to be held more than the retention period referred to in 7.1, the Principal or their nominated deputy will be responsible for authorising such a request. A record of these stored images will be kept within the CCTV viewing log.

7.4 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. The CCTV monitoring log will provide evidence of the images which have been held and where they are kept. When deleted this will be recorded in the CCTV monitoring log.

7.5 Access to retained CCTV images is restricted to the Principal and other persons as required and as authorised by the Principal. These individuals are: Assistant Principals, Principal, Office Manager, Vice Principal, Cluster Facilities Manager, Senior Network IT Technician

8. Complaints procedure

8.1 Complaints concerning the Academy's use of its CCTV system or the disclosure of CCTV images must be made in writing to the Principal at Sedgehill Academy, SE6 3QN. Any complaint will be handled in accordance with the Academy's complaints policy.

8.2 All appeals against the decision of the Principal must be made in writing to the Chair of Governors.

9. Monitoring Compliance

9.1 All staff involved in the operation of the Academy's CCTV System must be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.

9.2 All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to have undertaken United Learning Data Protection training.

10. Policy review

10.1 The Academy's usage of CCTV and the content of this policy shall be reviewed annually by the Governing Body with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.