CCTV POLICY

Contents

Policy Statement (1)

Policy Statement (2)

Key Personnel

CCTV system overview

Purposes of the CCTV system

Monitoring and recording

Compliance with Data Protection legislation

Applications for disclosure of images

Retention of images

Complaints Procedure

Monitoring compliance

Policy Statement (1)

As part of United Learning, the school adheres to all Group policies and procedures with relation to data protection and is mindful of national guidance for schools on this and related issues. AKS Lytham 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 school and details the procedures to be followed in order to ensure that the School complies with relevant legislation and the current Information Commissioner's Office Code of Practice.

The school 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 school 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.

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).

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

This policy and the procedures therein detailed, applies to all the School's CCTV systems.

Policy Statement (2)

1. This policy applies to all members of the AKS school community, including those in our EYFS setting.
2. AKS implements this policy through adherence to the procedures set out in the rest of this document.
3. This policy is made available to all interested parties in accordance with our *Provision of Information* policy. It should be read in conjunction with the following policies: *Provision of Information* and *Data Protection Policy*.
4. The school is fully committed to ensuring that the application of this policy is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the school's *Equal Opportunity* policy document.
5. This policy is reviewed at least annually, or as events or legislation changes require, by the Whole School Leadership Team and the Local Governing Body. The deadline for the next review is no later than 12 months after the most recent review date.
6. This is a new policy on its first edition.

Key Personnel

1. David Harrow: Headmaster
2. Annie Millard: Director of Finance and Operations & Health & Safety Officer
3. Amanda Ilhan: Head of Nursery and Preparatory School
4. Allan McKeown: Senior Deputy Head
5. Phil Hayden: Deputy Head (Pastoral)
6. Katy Nicholson: Systems Manager
7. Robert Duncan: Head of Estates and Grounds

CCTV System Overview

The CCTV system is owned by AKS Lytham, Clifton Drive South, Lytham St Annes, FY8 1DT and managed by the school and its appointed agents. The data controller for CCTV images held by AKS Lytham is United Church Schools Trust (UCST). UCST is registered with the Information Commissioner's Office (ICO). The registration number is Z533407X.

The Group's Data Protection Officer is responsible for ensuring that UCST complies with the Data Protection Law. The Data Protection Officer 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.

AKS Lytham's designated Data Protection Lead 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.

The CCTV system operates across the school. Details of the number of cameras can be given on request. 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 school and a 24-hour contact number for the Security Control Centre is provided, if appropriate.

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

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

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

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

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

Purposes of the CCTV System

The principal purposes of the School'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 school regulations by staff or students.

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

The school 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.

Monitoring and Recording

Cameras are monitored in the school's technical services department, estates manager's office, the school's designated safeguarding lead and by the security officer.

Images are recorded centrally on servers located securely in the school's core server room and are viewable in technical services department, estates manager's office and by the security officer by all CCTV trained staff. Additional staff may be authorised by the headmaster to monitor cameras on a view only basis to support trained staff i.e. in identifying specific children.

Trained staff are as follows:

Katy Nicholson – Systems Manager
Andrew Parker – IT Technician
Robert Duncan– Head of Estates and Grounds
Philip Hayden – Deputy Head (Pastoral) and DSL

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 should 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 should not contain names, whether any images have been copied and where they have been copied to.

The cameras installed shall 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.

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 will be securely stored in either OneDrive or appropriate Teams area in accordance with the process outlined in the retention of images section.

The use of cameras placed in the front of the classroom to monitor student behaviour will be carried out in accordance with Part 3 of the Employment Practices Code. The monitoring of classrooms should be clearly identified in the Privacy Impact Assessment. This should cover:

- identifying clearly the purpose(s) behind the monitoring arrangement and the benefits it is likely to deliver.
- identifying any likely adverse impact of the monitoring arrangement
- considering alternatives to monitoring or different ways in which it might be carried out.
- taking into account the obligations that arise from monitoring.
- judging whether monitoring is justified.

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

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 should 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.

The use of covert cameras will be 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 Headmaster and DSL will be sought before the installation of any covert cameras. The Headmaster 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.

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.

Compliance with Data Protection Legislation

From 25 May 2018, the school will also comply with the General Data Protection Regulation. Due regard will be given to the data protection principles contained within Article 5 of the GDPR which provide that personal data shall be:

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.

All storage used for images, recorded or downloaded for investigations, must be in compliance with GDPR rules; on secure storage on premise or on cloud storage within the European Union.

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

Application for Disclosure of images

Applications by individual data subjects

Requests by individual data subjects for images relating to themselves, Subject Access Request, should be submitted in writing.

In order to locate the images on the school'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.

Where the School 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

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

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.

All unexpected requests for CCTV images by a third parties, including requests made by the police, should be referred to the School'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.

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

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

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.

Retention of Images

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.

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

Where an image is required to be held in excess of the retention period referred to above, the Headmaster 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.

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 should be recorded in the CCTV monitoring log.

Access to retained CCTV images is restricted to the Headmaster and other persons as required and as authorised by the Headmaster.

Complaints Procedure

Complaints concerning the school's use of its CCTV system or the disclosure of CCTV images should be made in writing to the Headmaster at AKS Lytham, Clifton Drive South, Lytham St Annes, FY8 1DT. Any complaint will be handled in accordance with the school's complaints policy.

Monitoring Compliance

All staff involved in the operation of the School's CCTV System will 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.

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

Updated	7th July 2026
Reason for changes	Annual review
Name of the owner	Katy Nicholson – Systems Manager
Audience	Staff
Location	Whole School Team
Review date	July 2027