Alexandra
Primary School

Aspire, Perform, Succeed

A policy for the use and monitoring of CCTV at APS

Drafted by: J Mansfield
Date: January 2022
Review: January 2023

Contents

1. Introduction

The purpose of this Policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at Alexandra Primary School. The school recognises that CCTV systems can be deemed to be intrusive of privacy.

However, the school uses CCTV for the purpose of a public task duty; the management and security of the site, monitoring health and safety and safeguarding of the pupils, parents, visitors and employees on site. By using CCTV, the school can monitor occurrences on site and also the security of the buildings and grounds.

All cameras can be monitored from the school business manager's office, the main school office and the Head Teachers office. Only designated staff can access the cameras, that is the Head Teacher, School Business Managed, Premises Managers and the IT lead.

The CCTV system is owned by APS, which is the data controller with regards to all images recorded. CCTV use is recorded in the school's entry as a data controller in the Information Commissioner's Office Data Protection Register, which may be accessed at ico.gov.uk. This policy complies with the General Data Protection Regulation.

2. Objectives of the CCTV system

The purpose of the CCTV system is to:

- To protect pupils, staff and visitors against harm to their person and / or property
- To increase a sense of personal safety and reduce the fear of crime
- To protect the school buildings and assets
- Without prejudice, to protect the personal property of pupils, staff and visitors
- To support the police in preventing and detecting crime
- To assist in identifying, apprehending and prosecuting offenders

- To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence
- To assist in managing the safe, orderly and inclusive school environment

The system will not be used to:

- Record sound.
- Provide recorded images for the world-wide-web.
- Carry out any function other than those specifically listed above.

3. Statement of Intent

CCTV Cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities, etc.

CCTV Cameras are installed in such a way that they are not hidden from view. Signs are predominantly displayed where relevant, so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used. Notification has been submitted to the Information Commissioner and the next renewal date has been recorded.

The CCTV system will seek to comply with the requirements both of the Data Protection Act and the most recent Commissioner's Code of Practice.

The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the system 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.

Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after an approximate period of 22 days, unless an incident has occurred on School premises and the footage is to be kept longer for a specific purpose.

This also can be shorter depending on storage space. CCTV footage is stored securely in a lockable office. If an incident has occurred, the footage in question should be stored securely in a way that maintains the integrity of the images pending further action. Once the action / investigation has been concluded, a review of the retention of the footage is exercised and secure, permanent disposal of the footage occurs when there is no longer a valid lawful basis to keep the images.

4. System Management

Access to the CCTV system and data shall be password protected and will be kept in a secure area.

The CCTV system will be administered and managed by the School Business Manager, K Griffiths, who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager, the system will be managed by John Norton, Headteacher. Mr. M Hughs, the schools IT / Systems lead, also manages the IT elements of the system.

The system and the data collected will only be available to the Systems Manager, their replacement and appropriate members of the senior leadership team as determined by the Headteacher.

The CCTV system is designed to be in operation for 24 hours each day, every day of the year, though the school does not guarantee that it will be working during these hours. It only records when motion is detected.

The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.

Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by proving clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those mentioned in paragraph above, requests access to the CCTV data or system, the System Manager must satisfy themselves of the identity and legitimacy of purpose of any person making such request. Where any doubt exists access will be refused. Details of all visits and visitors will be recorded in a system log book including time / date of access and details of images viewed and the purpose for so doing.

5. Downloading Captured Data on to Other Media

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures:

- Each downloaded media must be identified by a unique mark.
- Before use, each downloaded media must be cleaned of any previous recording.
- The System Manager will register the date and time of downloaded media insertion, including its reference.

- Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a downloaded media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.
- If downloaded media is archived the reference must be noted.
- If downloaded media is put onto a device, the device will be encrypted and password protected.

6. Access to and disclosure of images to third parties

Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, the Headteacher and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the school, and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The school also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the school to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the police.

Applications received from outside bodies (e.g. solicitors or parents) to view or release images will be referred to the school's Data Protection Officer and a decision made by a senior leader of the school in consultation with the school's data protection officer.

7. Requests for Access by the Data Subject

Individuals have the right to request access to CCTV footage relating to themselves under the GDPR and DPA. The Subject Access and ICO guidance will be followed.

All requests should be made in writing to the Headteacher. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

The School will respond to a request within one calendar month of receiving a valid request.
Where a Subject Access Request includes footage of another individual not included in the request, the school must either use 'blurring' to distort the images to only the relevant individual, or gain consent to disclose third party personal data from those individuals not involved in the request.

The School reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

Wherever possible, the School will notify the requester if an exemption or limitation to their request applies, such as, but not limited to:

- A claim to legal professional privilege in legal proceedings
- The request will infringe on a third party's rights and freedoms
- Any other exemption to the right of access as stated in the GDPR and DPA.

The School understands that individuals have further individual rights under the GDPR and Data Protection Act and will seek DPO (Data Protection Officer) advice where necessary.

The Data Protection Act provides Data Subjects – those whose image has been captured by the CCTV system and can be identified - with a right to access data held about themselves, including those obtained by CCTV. Requests for such data should be made to the Headteacher.

8. Public information

Copies of this policy will be available upon request from the school office and posted on the school website.

9. Breaches of Policy

Any breach of policy by school staff will be initially investigated by the Headteacher, in order for them to take the appropriate disciplinary action. Any loss or unauthorised access to CCTV systems or footage should be managed in accordance with the school Data Security Breach Incident Management Policy.

10. Complaints

Any complaints about the school's CCTV system should be addressed to the Headteacher. Complaints and enquiries about the operation of CCTV within the school should be addressed through the School's complaints procedure, available on the school's website. Where necessary, the School's Data Protection Officer will be informed of the complaint.

11. Review of policy

The School's Data Protection Officer, Head Teacher will review this document annually to reflect changes in best practice, legislative changes and guidance from the Regulatory Authority (Information Commissioner's Office). Changes will be ratified by the Governing Board.

12. Summary of Key Points

- This Policy will be reviewed annually.
- The CCTV system is supplied by ADT but operated by the school.

- The SBM office is not open to visitors except by prior arrangement and good reason.
- Liaison meetings may be held with the Police and other bodies.
- The system may only be viewed by Authorised School Officers, system approved staff and the Police.
- Copies will not be made available to the media for commercial or entertainment purposes.
- Copies will be disposed of securely by destruction via shredder.
- Any breaches of this policy will be reported to and investigated by the Headteacher. An independent investigation will be carried out for serious breaches.

13. This policy links to the following other school policies:

Data Security Breach
Data Protection
Anti-Bullying
Attendance
Complaints
Designated Teacher for Looked After and Previously Looked After Children
Equalities
Exclusion
Medical
Rights Respecting
Safeguarding and Child protection
SEND
Staff Code of Conduct
Whistle Blowing
Whole, Happy, Healthy Strategy