CCTV Policy

Esh Winning Primary School

Policy Date:	18th Oct 2023
Next Review Date:	Oct 2024

Contents

1. Introduction
2. Scope
3. Roles and Responsibilities
4. System Description
5. Covert Recordings
6. Operating Standards
7. Retention of images
8. Data Subjects Rights
9. Access to and disclosure of images to third parties
10. Complaints
11. Policy Review

1. Introduction

1.1 Esh Winning Primary School operates a Closed-Circuit Television (CCTV) System.

1.2 The purpose of this Policy is to ensure that the CCTV system used at Esh Winning Primary School is operated, used and managed in accordance with the requirements of the Data Protection Act 2018 ('the DPA 2018), of the General Data Protection Regulation ("GDPR") and includes the principles governing the processing of personal data as set out in Appendix 1. It also seeks to ensure compliance with all privacy laws, including the Human Rights Act, the Regulation of Investigatory Powers Act 2000 and takes into account best practice as set out in CCTV codes of practice issued by the Information Commissioner and the Surveillance Camera Commissioner.

1.3 Esh Winning Primary School uses CCTV only where it is necessary and propionate for the following legitimate purposes:

- protecting school buildings and assets from damage, disruption, vandalism and other crime;
- to act as a deterrent against crime;
- promoting the health and safety of staff, pupils and visitors, including for monitoring student behaviour;
- to support the Police and other law enforcement bodies in the prevention, detection and prosecution of crime;
- to assist with the identification and apprehension of offenders; and
- to assist in the investigation of breaches of school policies and codes of conduct by staff, students, and where relevant investigating complaints.

1.4 This policy will be reviewed annually by the Governing Body to assess compliance with paragraphs 1.2 and 1.3 and to determine whether the use of the CCTV system remains justified, necessary and proportionate.

1.5 In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

2. Scope

2.1 This policy applies to the CCTV system in operation across the school site.

2.2 This policy applies to all Esh Winning Primary School staff, contractors and agents who operate, or supervise the operation of, the CCTV system.

2.3 This policy must be read in conjunction with the School's:

- Data Protection Policy

3. Roles and Responsibilities

3.1 The Governing Body of Esh Winning Primary School (the Data Controller) has overall legally responsibility for this policy but has delegated day-to-day responsibility for overseeing its implementation to the staff identified in this policy. All relevant members of staff have been made aware of the policy and have received appropriate training.

3.2 The Headteacher is responsible for:

3.2.1 ensuring that the CCTV system including camera specifications and locations for new and existing installations complies with the law and best practice referred to in clause 1.2 of this policy. Where new surveillance systems are proposed, the Headteacher will consult with the Data Protection Officer to determine whether a Data Protection Impact Assessment is required in accordance with the requirements of the GPDR;

3.2.2 the evaluation and chosen location where live and historical CCTV recordings are made available for viewing.

3.2.3 Ensuring access to the CCTV system is restricted to authorised staff only.

3.2.4 Maintaining a record of all access to the CCTV system i.e. an access log.

3.2.5 Maintaining a record of the disclosure of any CCTV images and recordings stored in the system to data subjects and/or third parties.

3.2.6 Ensuring all CCTV images and recordings stored on removeable media such as DVD, CD, tapes etc, are held in a secure location, with access to the removable media restricted to authorised staff only.

3.2.7 Ensuring that CCTV images and recorded footage stored on DVD, CD, tapes are not duplicated for release / disclosure.

3.2.8 Ensuring that the disclosure of any recorded CCTV material to data subjects and third parties is done so in compliance with this policy;

3.2.9 Ensuring that CCTV images and recordings are stored for a period not longer than 31 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Headteacher.

3.2.10 Ensuring that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy.

3.2.11 Ensuring that all access to the CCTV system and the cameras is only used to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.

3.3 Only the school's appointed contractor for the CCTV system is authorised to install, service and/or maintain it.

3.4 Changes in the use of the CCTV system can be implemented only by the Headteacher in consultation with the Data Protection Officer.

3.5 The Data Protection Officer is responsible for monitoring this policy and for providing data protection advice and guidance.

4. System Description

4.1 The CCTV system covers:

- building entrances,
- car parks, perimeters,
- external areas such as school yard, playing field
- internal social areas such as cloakrooms and the Reception foyer

The CCTV System continuously record activities in these areas 24 hours a day, seven days a week, and some of the cameras are set to motion detection.

4.2 The fixed location and positioning of CCTV cameras is chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. The school make every effort to locate and position CCTV cameras so that their coverage is restricted to the school site, which includes both indoor and outdoor areas. As far as practically possible, CCTV cameras will not focus on private homes, gardens or other areas of private property.

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

4.4 CCTV cameras are installed in such a way that they are not hidden from view.

4.5 The school will perform a Data Protection Impact Assessment when installing new fixed, or moving existing fixed, CCTV cameras to consider the privacy issues associated with using new and alternative camera locations and positions, to ensure the use continued use of the CCTV system is necessary and proportionate to address the legitimate purpose(s) set out at paragraph 1.3.

4.6 The CCTV system does not have sound recording capability.

4.7 CCTV Signage is prominently displayed across the site, both indoors and outdoors, so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signage contains the contact details for the school together with a description of the purposes for which CCTV is used and a contact telephone number.

4.8 The contact telephone indicated on the CCTV signage is available to members of the public during normal school hours. Employees staffing the contact telephone number point must be familiar with this policy and the procedures to be followed in the event that an access request is received from a Data Subject, the Police or any other third-party organisation.

5. Covert recording

5.1 Covert recording (i.e. recording which takes place without the individual's knowledge):

5.1.1 may only be undertaken in exceptional circumstances, for example to prevent or detect an unlawful act or other serious misconduct, and if is proportionate i.e. there is no other reasonable, less intrusive means of achieving those purposes;

5.1.2 may not be undertaken without the prior written authorisation of the Headteacher. The Headteacher will consult with the Data Protection Officer before undertaking any covert recording. All decisions to engage or refuse in covert recording will be documented, including the reasons;

5.1.3 will focus only on the suspected unlawful activity or suspected serious misconduct and information obtained which is not relevant will be disregarded and where reasonably possible, deleted; and

5.1.4 will only be carried out for a limited and reasonable period consistent with particular purpose of the recording and will not continue after the investigation is completed.

6. Operating Standards

6.1 The operation of the CCTV system will be conducted in accordance with this policy.

6.2 No unauthorised access to the CCTV system will be permitted at any time.

6.3 Other than the Headteacher, access to the CCTV system will be limited to:

- persons specifically authorised by the Headteacher;
- The Data Protection Officer
- authorised maintenance engineers;
- police officers where appropriate; and
- any other person with statutory powers of entry

6.4 CCTV Monitors are not visible from outside the Server Room where they are located. The location of CCTV monitors has been chosen to ensure images displayed are not visible to pupils, unauthorised staff, visitors and members of the public.

6.5 Before permitting access to any part of the CCTV system, the Headteacher will take all necessary steps to verify the identity of any visitor and establish the existence of the appropriate authorisation. All visitors are required to complete and sign the visitors' log, which includes details of their name, department and/or the organisation that they represent, the name of the person they are visiting and the reason for the visit.

6.6 A CCTV access log is maintained and securely retained by the Headteacher which includes the following information:

- person reviewing recorded footage;
- time, date and location of footage being reviewed; and
- purpose of reviewing the recordings.

6.7 CCTV images and recordings will be displayed only to persons authorised to view them or to persons who otherwise have a right of access to them. Where authorised persons access or monitor CCTV images on workstation desktops, they must ensure that images are not visible to unauthorised persons for example by minimising screens when not in use or when unauthorised persons are present. Workstation screens must always be locked when unattended.

6.8 Images produced by the recording equipment must be as clear as possible, so they are effective for the purpose for which they are intended. The standards to be met in line with the codes of practice referred to paragraph 1 of this policy are set out below:

- recording features such as the location of the camera and/or date and time reference must be accurate and maintained;

- cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established;
- consideration must be given to the physical conditions in which the cameras are located i.e. additional lighting or infrared equipment may need to be installed in poorly lit areas;
- cameras must be properly maintained and serviced to ensure that clear images are recorded, and a log of all maintenance activities kept; and
- as far as practical, cameras must be protected from vandalism in order to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit within a vandal resistant casing.

7. Retention of images

7.1 CCTV images are not to be retained for longer than necessary, taking into account the purposes for which they are being processed. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce an approximate 30-day rotation in data retention.

7.2 Provided that there is no legitimate reason for retaining the CCTV images (such as for use in disciplinary and/or legal proceedings), the images will be erased following the expiration of the retention period.

7.3 All retained CCTV images and recordings stored on removeable media will be stored securely, with access restricted to authorised staff only.

8. Data Subjects Rights

8.1 Recorded images of (identifiable) individuals are personal data of the individuals (Data Subjects) whose images have been recorded by the CCTV system.

8.2 Data Subjects have a right of Access to the personal data under the DPA 2018 and the GDPR. They also have other rights under the DPA 2018 and the GDPR in certain limited circumstances, including the right to have their personal data erased, rectified, to restrict processing and to object to the processing of their personal data.

8.3 Requests by Data Subjects for CCTV images and recordings relating to themselves (Subject Access Request) should be submitted in writing to the school together with proof of identification such as a passport or driving licence along with proof of address.

8.4 In order to locate the images on the CCTV 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.

8.5 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.

8.6 The school will respond to a Subject Access Request within one month of receiving the request. This includes a request received in school during school holidays.

8.7 The period for responding to the request may be extended by two further months where necessary, taking into account the complexity and number of the requests. The school will notify the Data Subject of any such extension within one month of receipt of the request together with the reasons for this.

9. Access to and disclosure of images to third parties

9.1 A request for images made by the Police or a third-party organisation, for example an Insurance company, should be made in writing to the school. The school will consult with its Data Protection Officer in relation to any request received from the police or a third-party organisation.

9.2 Legal representatives making subject access request on behalf of a Data Subject will be required to submit a letter of authority to act on behalf of the Data Subject together with the evidence of the Data Subject's identity, the reason(s) for the request, and the lawful authority under which the request is being made.

9.3 In limited circumstances it may be appropriate to disclose CCTV images and recordings 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.

9.4 Such disclosures will be made at the discretion of the Headteacher, with reference to relevant legislation and where necessary, following advice from the school's Data Protection Officer.

9.5 Where a suspicion of misconduct arises, the headteacher of school may provide access to CCTV images for use in staff disciplinary cases. The Headteacher will consult with the Data Protection Officer in relation to an Requests for CCTV images and recordings requested or required for staff or student disciplinary purposes or complaints

9.6 The Headteacher may provide access to CCTV images to Investigating Officers when sought as evidence in relation to student discipline cases.

9.7 Every disclosure of CCTV images and recordings is recorded by the Headteacher in an access log containing the following information:

- the name of the police officer or other relevant person in the case of other agencies/bodies receiving the copy of the recording;
- brief details of the images captured by the CCTV to be used in evidence or for other purposes permitted by this policy;
- the crime reference number where relevant; and
- date and time the images were handed over to the police or other body/ agency.

10. Complaints

10.1 Any complaints relating to the operation, use and management of the CCTV system should be in writing to the Data Protection Officer at the following address:

Data2Action
Suite 2e
Innovator House
Silverbriar
Sunderland
SR5 2TP

Email: SchoolsDPO@data2action.co.uk
Telephone: 03332026397

10.2 A complaint will be responded to within a month following the date of its receipt. Records of all complaints and any follow-up action will be maintained by the Data Protection Officer

11. Policy Review

11.1 This policy will be reviewed annually by the Governing Body to assess compliance with paragraphs 1.2 and 1.3 and to determine whether the use of the CCTV system remains justified, necessary and proportionate.

11.2 In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

Appendix 1

Principles relating to the processing of personal data under the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the Data Subject;

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; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of 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 unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.