SPRINGVALE
Primary School

PLAYLEARNACHIEVETOGETHER

Policy:

CCTV Building and Security

Approved by the governing body on.....

Play together, learn together, achieve together.

SPRINGVALE PRIMARY SCHOOL

CCTV Building and Security Policy

Introduction

This policy has been formally adopted by the governors of Springvale Primary School.

Aims and Principles

The policy is underpinned by the central aims of Springvale Primary and values held by the school community:

Aims of the school

- Springvale is committed to promoting high standards of academic achievement for all learners in all subjects.
- As a school we will continue to develop and instil key life skills and values in our pupils.
- We will encourage positive relationships and communications between home, our community and the wider world.

In particular, Springvale School has an inclusive approach to our provision. Our aim is always to involve all our children and stakeholders in all areas of the curriculum and school life. In accordance with our **Disability Equality Scheme** we recognise that this may mean making special adaptations or arrangements from time to time for children with specific disabilities. We welcome the involvement of disabled adults in all areas of school life.

Background Information

Springvale Primary School is a caring and open school, where parents, children, staff and the wider school community all know that their views and needs will be listened to, in both education and personal areas.

Key authorising signatories to the PFI Primary Project CCTV code of practice.

Springvale Primary ……..…… Date ……..

Modern Schools Barnsley……Date ……

Barnsley MBC ……...…….. … Date ……..

ENGIE PLC …….. Date ……...

Contents

Definitions

Data Controller:- A person who determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Processor:- Any person (other than an employee of the data controller) who processes the personal data on behalf of the data controller.

Additional GDPR information for schools available on the IOC website: https://ico.org.uk/for-organisations/education/ **INTRODUCTION**

The principles of operating a CCTV system

Closed Circuit Television (CCTV) is a method of observing places and people, usually from a distance. It comprises of one or more cameras viewing a 'scene' and displaying that scene to a CCTV operator on a monitor screen. The images viewed may be recorded for later playback. This Code of Practice is concerned only with recorded images that can be retrieved on demand at a later date.

CCTV surveillance is an increasing feature of our daily lives and could intrude into our private lives. Therefore for public confidence and to meet legislative requirements the schools CCTV system needs to be managed.

This document sets out the accepted use and management of the CCTV system and images to ensure the compliance with the General Data Protection Regulation (GDPR) and associated legislation ('data privacy legislation'), the Human Rights Act 1998 (HRA), the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act (POFA Code) and other legislation.
Where images are 'real time' and not recorded then the Data Protection Act does not apply, but other legislation or policies may.

This document relates only to CCTV systems that operated within the PFI Primary School Project. This document is intended to add detail to the various contracts which link the different parties together:

- Project Agreement dated 4th May 2005 between Barnsley Metropolitan Borough Council (BMBC) and Modern Schools Barnsley Ltd (MSB)
- Governors agreement dated 4th May 2005 between School and Barnsley metropolitan Borough Council (delate for Academy policy) School Agreement between……..Academy Trust and Barnsley Metropolitan Borough Council dated ……(delate for maintained school policy)
- Facilities Management Agreement dated ……. Between Modern Schools Barnsley Ltd and ENGIE Services Ltd (ENGIE).

It does not cover –

- Targeted and Intrusive Surveillance Activities which are covered by the Regulation of Investigatory Powers Act (RIPA).
- Use of surveillance techniques to monitor employees' compliance with their contracts of employment if any such surveillance exists.
- Use of cameras and similar equipment by the media for the purposes of journalism, or for artistic or literary purposes.

The framework for a CCTV policy is based on –

- The legality of the CCTV system.
- The training of managers and employees.
- The set up and operation of the CCTV system.
- The rights of the public with relation to recorded images.

The CCTV operating system is the property of Modern Schools Barnsley Ltd (MSB) while all rights in the material recorded using the CCTV equipment (including any copies of such material or images extracted from it) shall automatically vest in and remain the property of the school. The schools facilities management provider ENGIE Ltd will undertake the day to day operation of the System to enable them to provide a safe secure environment for all users of the school Facility in line with the PFI Project agreement dated 4th May 2005.

The individual school will be considered Data Controllers and as such have a duty to comply with the principles as set out in Data Protection Legislation including Data Protection Act 2018 and the General Data Protection Regulations.

ENGIE Ltd will be considered Data Processor and as such have a duty to comply with the data protection principles set out in Data Protection Legislation. ENGIE Ltd will support the schools operation of the CCTV system as and when required by school:-

- Assisting in the retrieval of images.
- Out of school hours monitoring and security call out (reviewing footage on activation).
- Editing images if required or appropriate.
- Maintaining:-
    - CCTV system
    - The record sheets with in this document i.e. access control, maintenance, incidents, etc.

The Parties have considered the appropriate legislation and considers the CCTV System compliant, meeting the requirements as prescribed by data protection legislation.

The CCTV scheme has been registered with the Information Commissioner under the terms of the Data Protection Act 2018 and General Data Protection Regulation and will seek to comply with the requirements of the Commissioners CCTV Code of Practice

Schools IOC Registration Number ……

General Data Protection Regulations Principals:-

These principles are broadly similar to the principles in the Data Protection Act 1998 (the 1998 Act).

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

Pseudonymisation

a.	processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
b.	collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
c.	adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
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 ('accuracy');
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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
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 ('integrity and confidentiality')."

THE SPRINGVALE PRIMARY SCHOOL CCTV SYSTEM

Responsibilities

The CCTV system installed at Springvale Primary School is operated by:-

1. Springvale Primary School (during school opening hours)

Responsibilities include operation while school open to staff and or pupils; representing the system in case of legal action being taken by plaintiffs.

The operation of this CCTV system, the procedures, staff training and responsibilities are in accordance with the Data Protection Legislation and any policies of Springvale Primary School.

The individual responsible for the CCTV system the Head Teacher

2. Modern School Barnsley (when school closed)

In line with the requirements of PFI primary school Project Agreement dated 4th May 2005 MSB's responsibilities include: specifying system specification; ensuring legal conformity to installation and operation when school closed to staff and/or pupils; representing the system in case of legal action being taken by plaintiffs.

The operation when school closed will be undertaken on behalf of MSB by the schools facilities management provider ENGIE. Should MSB wish to view or use any captured images a formal request will be made to the Data Controller using Access Request (SAR) form appended to this document.
Under the terms of PFI Project Agreement dated 4th May 2005 the individual responsible for the CCTV system is the General Manager of MSB.

Authorised visitors are:-

Third party authorised visitors must have appropriate licence to view/process images and require written authorisation (email) from the schools head teacher and/or Project Director of MSB on each occasion.

Maintenance Engineer approved (appropriately licenced) and appointed by ENGIE on behalf of MSB. Note: Maintenance log in TAB 2 must be completed

Operational Control Contacts

Operational Control	Address	Reason	Contact
ENGIE Services Ltd c/o Modern Schools Barnsley (out of school hours)	Park St Primary School (FM Office) Barnsley S730HS	Prevention & detection of crime, safety of pupils and staff	03336660122
Springvale Primary School	Royston road Cudworth Barnsley s720EQ		01226 719700

Purpose of the CCTV System:-

- Safety & security of employees, pupils, contractors and visitors.
- Security of premises during and outside normal working hours.
- Car park monitoring.
- Prevention, investigation and detection of crime.

Important Notes:

- CCTV systems must not be used for general surveillance of staff or visitors or for purposes not compatible with the purposes indicated above.
- Where law enforcement organisations request control of the system (e.g. to mount a specific surveillance operation) then the CCTV Manager will ensure that s/he is satisfied as to the legality of the request and that appropriate documentation and controls are in force to maintain the basic operational principles of CCTV usage.
- The CCTV system is not intended to be constantly monitored. Relevant Health & Safety considerations shall be applied in accordance with current guidance or directive e.g. s at 31st January 2006 unbroken viewing of a monitor screen usually attracts a 'change of duties' period of 10 minutes in every hour.

The CCTV system has no audio recording function should this change the policy shall be reviewed and updated to reflect the new requirement?

- .

Retention Period

The retention period needs to be suitable for the purpose and images should not be kept any longer than considered necessary. Data captured on the will be kept for:-

- Routine recorded footage 30 days at which point the system will automatically delete the data. This is considered to be a reasonable length of time for incidents to be identified, investigated and allows sufficient time to process any subject access requests (SAR's).
- Retrieved images:-
  - Retention polices should be referred to for guidance relating to any retrieved images.
  - IF NOT SURE advice should be sought via the individuals responsible for the CCTV system before deleting images that may have future legal or insurance implications.
  - Note: For the remained of the PFI project ALL named responsible persons for the CCTV system must issue written approval to other before any retrieved images are delated. This written approval/denial should contain the reasons for keeping or deleting the images.
  - Actions should be recorded in "Record Log of CCTV Viewing / Removal of Recorded Images".
- In certain circumstances where SAR or an incident has occurred it may be prudent to retrieve and save data documenting the reasons until such time as the matter has been resolved?

Access to and disclosure of images to third parties

Access to & disclosure of images to third parties must be for valid, documented and reasoned:-

Restricted access to image recordings, their disclosure to third parties and the quality of the images disclosed are subject to the organisation's policy which has reference to the Data Protection Principles. And where appropriate in line with GPDR principles that inform individual's rights to the data being processed about them.

People whose images are recorded have the right of Subject Access. It does not refer to people who request information that contains images of other people - that is a Freedom of Information request.

CCTV managers, operational staff and admin support staff must be able to recognise a Data Protection Subject Access Request (SAR) ref 3.8.1.6 for standard SAR.

Such a SAR request may not be titled Data Protection, or may be incorrectly titled as Freedom of Information Request. We need to decide which it is and process the request according to the appropriate legislative rules. Where this has been requested it is important that all images of other data subjects are redacted before issuing...

All requests for access should be recorded, stating if disclosure has been made or not, a response needs to be within 1 calendar month of the request and subsequent updates should additional information be requested.

Images should be restricted to authorised persons; monitors should be turned and password protected while un-authorised visitors are in control room i.e. cleaners etc.

Third parties

GDPR says you do not have to comply with a SAR if to do so would mean disclosing information about another individual who can be identified from that information, except where:

- the other individual has consented to the disclosure; or
- it is reasonable in all the circumstances to comply with the request without that individual's consent.

So, although you may sometimes be able to disclose information relating to a third party, you need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. If the other person consents to you disclosing the information about them, it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

Making decisions about disclosing third-party information should be made on a case-by-case basis. We must not apply a blanket policy of withholding it.

Refer to IOC website for further advice and information where the request includes a third party. https://www.itgovernance.eu/blog/en/how-will-the-gdpr-affect-cctv-and-workplace-monitoring/

Subject Access Request (SAR) (Application form)

Applicant must submit a request in writing. This can be through their own written request but it must contain the necessary information that facilitates the search for information e.g. images at a certain place, date and time or via the standard form contained within this policy.

Review procedures

This policy should come into effect as the new CCTV system comes into use in 2018 and should be reviewed annually by operators and by the PFI project team following any changes or an incident that material impacts on the system and/or its operation.

Additional Information Relevant to CCTV and Data Protection

Additional information and guidance can be found on the ICO website:-

Home page-https://ico.org.uk/

CCTV Code of Practice-https://ico.org.uk/media/about-the-ico/consultations/2044/draft-cctv-cop.pdf

Preparing for General Data Protection Regulations (GDPR)- https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

SIA Licence Advice https://www.gov.uk/public-space-surveillance-cctv-licence

TAB 1 Installation, Maintenance and Training (includes maintenance and authorised access logs).

Installation and Maintenance Check List

The Quality of images must be fit for the system purpose failure to produce adequate images for the stated purpose of the system breaches GDPR & Data Protection Act 2018.		
		Yes/No/Comments
1.	Upon installation does the system perform properly?	(c,d,e)
2.	Is all equipment sited in such a way that it only monitors those areas that are intended to be covered by the equipment and or have measures to prevent images being captured within neighbouring sites?	(b,e)
3.	Siting of monitor for live images positioned to prevent individuals being identifiable by un-authorised people (not easily visible from reception desk).	
3.	Are cameras protected where necessary e.g. from vandalism - by being boxed in, out of reach.	
4.	If the system records location/date/time is this information accurate?	(d)
5.	Can the system be searched using records location/date/time?	
5.	Are system operation instructions available for operators?	
6.	Does a regular maintenance/service schedule of the system exist to ensure clarity of pictures is a maintenance log kept?	
7.	Are adjustable cameras restricted to prevent surveillance of areas not designated for such?	
8.	Is signage (for overt surveillance) clearly visible? The signs must - • Identify the responsible person and/or organisation [e.g. Name of School] • The purpose of the scheme [e.g. Prevention and detection of crime] • Details of whom to contact regarding the scheme [e.g. Barnsley FM 03336660122] The signs (and wording) must be of an appropriate size.	(a)
9.	If a camera is damaged is there a clear procedure for:- • Defining the person responsible for making arrangements for camera repair. • Ensuring the camera is fixed within a specific time. • Checking the quality of the maintenance work.	(d)

School Operator Check List

School and Remote Operators		
		Y/N/Comments
1.	Have operators received adequate training relating to reviewing and retrieving images?	(f)
2.	Are operators aware of the purpose of the surveillance (which will guide their actions)?	
3.	Are operators trained in recognising the privacy implications of surveying such areas i.e. implication for neighbours?	(a, b, c, d, e & f)
4.	Are operatives aware of:- • This policy? • GDPR Principals listed in this policy? • Their responsibility in relation to:- ○ Reporting faults including blurred images to the FM help desk ○ Recording any CCTV Maintenance in the maintenance log records? ○ Subject Access Requests and the policy standard form and how to use it? ○ Log of access ○ Control Room access protocol?	
5	Are monitors turned off and password protected when unauthorised persons in the control room i.e. visitors, cleaners, maintenance staff etc.	

CCTV Maintenance Log (Ref to O&M manual for manufactures and installer information)

The equipment should be constantly monitored for effective operation and any problems reported immediately to FM help desk.

Date Reported	Camera No.	Fault Details/ Action Taken	Date Repaired

CCTV Control Room list authorised persons (Authorised to access this area)

All listed persons must be in possession of this CCTV Code of Practice and have the facility to query any aspect of the CCTV operation they are not clear about.

Persons listed below are authorised to access the schools main admin office containing CCTV controls with good reason to do so. All other persons to sign CCTV Control Room Record of Visitors sheet contained within this policy stating name, position, date, time and reason for being in the area or system should be securely isolated to prevent viewing access while visitor present.

Name (print)	Position	Date issued with CCTV Code of Practice
All teaching and administration staff	**Directly Employed by School**	

TAB 2 Subject Access Requests (SRA) forms, check sheets and record logs.

PFI PRIMARY SCHOOL SUBJECT ACCESS REQUEST (SAR)

Data Protection Act 2018
APPLICATION FOR INFORMATION CCTV IMAGES

- Please complete the form as fully as possible.
- You may be asked to supply evidence of your identity e.g. driving licence, passport or utility bills in your name/address.
- If you are asking for footage about someone else you must have written permission from them giving the authority for you to do so.

SECTION 1 – YOUR DETAILS

First name(s)		**Last name**	
Address			
Post code			
E-mail address			
Telephone no.			

SECTION 2 – DETAILS OF DATA SUBJECT IN CCTV FOOTAGE (if different from above)

First name(s)		**Last name**	
Address			
Post code			

Please note that if you are not the subject of the CCTV footage you must provide evidence that you have permission to ask for it e.g. a letter of authorisation or Power of Attorney etc. (Please send a copy with this request)

SECTION 3 – AGENCY OR REPRESENTATION DETAILS (Please tick if appropriate and supply documentation of which exemption under the Data Protection Act 2018 you wish to apply)

Do you represent the police and the images are required to prevent/detect a crime?	
Do you represent a prosecution agency and require the images to prosecute an offender?	
Are you a solicitor or barrister and require the images in connection with legal proceedings?	
Do you represent the media, where disclosure of the image to the public is needed in order to assist in the identification of a victim, witness or perpetrator in relation to a criminal incident?	

SECTION 4 – DETAILS OF REQUIRED IMAGES (Please provide the following information to assist in the search for CCTV images)					
Date image was recorded		**Time image was recorded (within 15 mins)**			
Location of footage (street, building, other landmark)					
Please provide a description of the incident you wish to view					
Please provide a photograph of yourself (or the subject), or a description, that will enable the operator to identify you/them on the CCTV footage	**Photograph provided? (please circle as appropriate)**	**Yes** **No**			
Do you want to view the footage in person? **(please circle as appropriate)**	**Yes** **No**	**Do you want a still image from the footage?** **(please circle as appropriate)**	**Yes** **No**		

Signature of subject at Section 1…… Date……

Signature of subject at Section 2…… Date……

(if applicable)

IMPORTANT INFORMATION:
Presentation of all original documentation, for example, proof of identity, letter of authorisation, will be required at the point of release of CCTV footage.

Please return this form by email to INSERT SCHOOL EMAIL or by mail to: INSERT SCHOOL ADDRESS...

Record Log of CCTV Viewing / Removal of Recorded Images

Staff should also record any incident viewed as an aid to subsequent investigations and report to management e.g. a car parking collision, visitor slipping on ice etc. even if the viewing resulted in no relevant images being observed/retrieved.

NOTE: One record per sheet to help maintain privacy.

Date & Time of Removal & Viewing	Date & Time of any Image Return	Name of Officer Providing or Removing Images	Person Taking or Viewing Images	Reason for taking or viewing Images (include location, camera number, date time etc.)	Outcome (if any)
		Print: **……** **Sign:** **……**	**Print:** **……** **Sign:** **……**		

PROCESSING THE IMAGES

Processing of personal images must conform to Data Protection principles:-		
		Yes/No/Comments
1.	Does an image retention policy exist - that not only states the length of time images should be retained but encompasses an active schedule for deleting images. Note: any retention policy should be included or referenced in this Code of Practice.	(c & d)
2.	Where images are retained is the reason for so doing documented? Note: The following must be recorded:- • Date of retention decision/action. • The reason for retention. • Any reference number e.g. crime incident number • Location of the images	(b, c & e)
3.	Are retained images stored in a secure place, access to which is controlled?	(f)
4.	Are surveillance monitors only viewable by authorised people?	
5.	Are all access requests controlled by an authorised person or persons?	(a, e & f)
6.	Is there an appropriate viewing area where only authorised people can see the images?	
7.	Where images are removed from the system for viewing is there a system for recording:- • Date and time of removal. • Name of person removing the images. • Name (and organisation) of any person viewing the images. • The reason for viewing. • The outcome, if any, of the viewing. • Date and time of return of the images to the system or secure place if images are retained further.	(a, e & f)
8.	Do system users know the procedures applicable to accessing recorded images?	
9.	Are procedures in place to train all operators in:- • System use responsibilities? • System users disclosure policy • Rights of individuals in relation to their recorded images.	(f)

CHECKLIST ACCESS/DISCLOSURE OF IMAGES TO THIRD PARTIES

Disclosure of images to third parties must be for valid and legal reasons and documented		
		Yes/No/Comments
1.	Is access to the images restricted to authorised persons?	(e & f)
2.	Are procedures in place to document any access to image recordings?	
3.	Are disclosure rules documented? Disclosure should only be made in limited and prescribed circumstances e.g. if disclosed for prevention & detection of crime then likely recipients are: the Police; prosecution agencies; legal representatives. Either a data sharing agreement should be in place or each disclosure covered by a Section 29(3) request form.	(a &f)
4.	Are all requests for access recorded - even if disclosure is not made?	
5.	Where access is allowed is the following recorded - • Date and time access allowed or images disclosed. • Identity of third party allowed viewing or receiving images. • The reason for allowing access. • Extent of the images/information disclosed.	(a, d ,e & f)
6.	Are images that should not be made widely available documented e.g. those not for disclosure to the media?	
7.	Are reasons for making images widely available documented	
8.	Can images be blurred before disclosure to a media company (requirement)? It may be necessary to identify an editing company who can do this.	(a & f)
9.	If an editing company is appointed:- • Does a contract exist between the CCTV owner, school (data controller) and the company? • Has the editing company given guarantees re security measures e.g. their staff vetting procedures, storage of images? • The CCTV owner should check that the guarantees are met? • Does the contract clearly state that the editing company can only use images in accordance with instructions of the CCTV owner? • Does the contract clearly state the security guarantee of the editing company?	(a & f)
10	If the media organisation is also the editing company the above will apply?	
11	Do all system users have an awareness of:- • Preventing processing likely to cause substantial or unwarranted	

	damage to an individual. • Preventing automated decision taking in relation to an individual.	
12	Is the person responsible for responding to SAR'S clearly identifiable to system users/operators	
13	In relation to a request to prevent processing (individual's right to request) is there a response process which clearly states whether or not the request will be complied with, and if not to be complied with states the reason(s)?	
14	Is there a procedure to ensure that a written response to a (3.) request, stating the decision, must be sent within 1 calendar month of receipt of the request? A copy of the response should be retained.	
15.	Is there a procedure to document:- • The original decision. • The request from the individual. • The response to the individual.	

Additional Notes: