



Inspire Partnership Academy Trust



Rockcliffe Manor Primary School CCTV Policy

Approved – July 2021

This is an approved template policy for adaptation in all Trust schools.

Table of Contents

1.	3	
2.	3	
3.	3	
4.	Monitoring of images	5
5.	Staff	5
6.	6	
7.	6	
8.	7	
9.	8	
10.	8	
Appendix 1		9
Appendix 2		11

1. Overview

- 1.1 Rockliffe Manor Primary School, part of the Inspire Partnership Academy Trust, has in place a CCTV surveillance system, "the system" within internal and external areas of the school site. Images are monitored and recorded centrally and will be used in strict accordance with this policy. The system is owned by the Inspire Partnership Academy Trust.
- 1.2 The Headteacher has initial responsibility for the operation of the system and for ensuring compliance with this policy and the procedures documented. They may be contacted as follows:

Nancy Cook: ncook@inspirerockliffe.co.uk

In the absence of the Headteacher this responsibility transfers to the Nominated Deputy. They may be contacted as follows:

William Connolly (Regional Facilities Manager): wconnolly@inspirepartnership.co.uk

General Data Protection Regulations: CCTV digital images, if they show a recognisable person, are personal data and are covered by the General Data Protection Regulations. This Policy is associated with the Inspire Partnership Academy Trust General Data Protection Policy, the provisions of which should be adhered to at all times.

2. The system

- 2.1 The system comprises of fixed position cameras only.
- 2.2 Cameras will be located at strategic points within the school site. No camera will be hidden from view. A list of locations is given at Appendix 1.
- 2.3 Signs will be prominently placed at strategic points and at entrance and exit points of the school site to inform staff, pupils, visitors, and members of the public that a CCTV installation is in use.
- 2.4 Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

3. Purpose of the system

3.1 The system has been installed with the primary purpose of reducing the threat of crime generally, protecting school premises and helping to ensure the safety of all staff, pupils, and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent or intent to abuse staff, pupils, or visitors physically or verbally.
- Assist in the prevention and detection of crime.
- Facilitate the identification, apprehension, and prosecution of offenders in relation to crime and public order.
- Support the school's statutory obligation to safeguard children.
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff and assist in providing evidence to managers and/or to a member of staff against whom disciplinary or other action is or is threatened to be taken.
- Facilitate the movement of vehicles on site.
- In the case of staff to provide management information relating to employee compliance with contracts of employment.

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

3.2 Covert recording

3.2.1 Covert cameras may be used under the following circumstances on the written authorisation or request of the DPO, CEO or COO and where it has been assessed re: General Data Protection Regulations by the DPO

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and

- That there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.

3.2.2 Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorised activity.

3.2.3 The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

4. Monitoring of images

4.1 Images captured by the system will be recorded via the recorder located in the main office with the monitor situated on top, twenty-four hours a day throughout the whole year. Monitors are sited as mentioned above and are not visible from outside the room.

4.2 No unauthorised access to the recording system will be permitted at any time. Access will be strictly limited to those expressly authorised by the headteacher/deputy headteacher, police officers and any other person with statutory powers of entry. A list of those members of staff authorised to access the Control Room is given at *Appendix 2*.

4.3 Staff, guests and visitors may be granted access to the recording system on a case-by-case basis and only then on written authorisation from the Headteacher. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter.

4.4 Before allowing access to the recording system, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation. All visitors will be required to complete and sign the visitors' log, located in the reception area, which shall include details of their name, their department or organisation they represent, the person who granted authorisation and the times of entry to and exit from the control room, this will also include any visitors granted emergency access.

5. Staff

- 5.1 All staff with authorised access to CCTV images will be made aware of the sensitivity of handling CCTV images and recordings. The Headteacher will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV.
- 5.2 Training in the requirements of the General Data Protection Regulations will be given to all those required to work in Rockliffe Manor school office.

6. Recording

- 6.1 Digital recordings are made using digital video recorders operating in time lapse mode. Incidents are recorded in real time.
- 6.2 Images will normally be retained for 30 days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.
- 6.3 All hard drives and recorders shall remain the property of the Inspire Partnership Academy Trust until disposal and destruction. *Method of destruction will be carried out by Plum Inovation . Hard drive will be wiped/destroyed.*

7. Access to images

- 7.1 All access to images will be recorded in an Access Log.
- 7.2 Access to images will be restricted to those staff who need to have access in accordance with the purposes of the system. A list of such staff is given at *Appendix 2*.
- 7.3 Access to images by third parties
 - 7.3.1 Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:
 - Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder.
 - Prosecution agencies
 - Relevant legal representatives

- The media where the assistance of the public is required in the identification of a victim of crime or the identification of a perpetrator of a crime.
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

7.4 Access to images by a subject

CCTV digital images, if they show a recognisable person, are personal data and are covered by the General Data Protection Regulations. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of the data, subject to exemptions contained in the Regulations. They do not have the right of instant access.

7.4.1 A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the DPO. Subject Access Request Forms are obtainable in hard copy from the school office. An electronic copy can be obtained via our website at <https://www.rockliffemanor.co.uk> or via email on info@inspirerockcliffe.co.uk A response will be provided promptly and in any event within 1 month of receiving the request.

7.4.2 The General Data Protection Act gives the DPO the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

7.4.3 If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing within 1 month, stating the reasons.

8. Complaints

8.1 It is recognised that some Data Subjects may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instance to the Headteacher Nancy Cook, on ncook@inspirerockcliffe.co.uk. Concerns or enquiries relating to the provisions of the General Data Protection Regulations and/or The Data Protection Act 2018 may also be addressed to the Trust CEO. These rights do not alter the existing rights of anyone under any relevant grievance or disciplinary procedures.

9. Data breach

- 9.1 A "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".
- 9.2 In the event that a data breach occurs, a thorough assessment of the breach will be made immediately by the Incident Response Team (IRT), comprised of the Headteacher, Trust COO and the DPO, and the Trust Data Breach Policy must be followed.
- 9.3 Immediate steps will be taken to ensure that the breach is contained, and the effects of the breach minimised and mitigated as much as possible.
- 9.4 If the data breach is deemed by the IRT to be reportable to the Information Commissioner's Office, the ICO will be notified within 72 hours of the discovery of the breach.
- 9.5 In the case of a serious breach, Data Subjects whose data has been affected will be notified, in writing.

10. Compliance monitoring

- 10.1 The contact point for staff or members of the public wishing to enquire about the system will be the Headteacher, by prior appointment.
- 10.2 Upon request enquirers will be provided with:
- A summary of this statement of policy
 - An access request form if required or requested.
 - A subject access request form if required or requested.
 - A copy of the Inspire Partnership Academy Trust's complaints procedures.
- 10.3 All documented procedures will be kept under review and a report periodically made to senior management.
- 10.4 The effectiveness of the system in meeting its purposes will be kept under review and reports submitted as required to senior management.

Appendix 1

Camera No.	Location	Type
1	Beachwood front entrance, carpark gate view	<i>Fixed Position, Infrared</i>
2	Front Entrance, carpark view	<i>Fixed Position, Infrared</i>
3	Front Entrance, Main door view	<i>Fixed Position, Infrared</i>
4	Front Entrance, side of building view	<i>Fixed Position, Infrared</i>
5		
6	Beachwood back of building, garden view	<i>Fixed Position, Infrared</i>
7	Beachwood front entrance, Beachwood front door view	<i>Fixed Position, Infrared</i>
8		
9		
10		
11		
12		
13		
14		

Appendix 2

Name	Job Title/Role	Contact Details
Nekema Douglas	Admin Assistant	ndouglas@inspirerockcliffe.co.uk
Kate Henderson	Admin Assistant	khenderson@inspirerockcliffe.co.uk
Sarah Sweet	Admin Manager	ssweet@inspirerockcliffe.co.uk