REDHILL ACADEMY TRUST

Equality and Achievement

CCTV POLICY

APPROVING BODY	TRUST EXECUTIVE BOARD
DATE APPROVED	November 2024
VERSION	2
SUPERSEDES VERSION	1
REVIEW DATE	OCTOBER 2025
FURTHER INFORMATION / GUIDANCE	Data Protection Act 2018 Equality Act 2018 General Data Protection Regulation 2018 Human Rights Act 1998 The Freedom of Information Act 2000

Contents

1. Aims

This policy aims to set out the school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property.

1.1 Statement of intent

The purpose of the CCTV system is to:

- Make members of the school community feel safe
- Protect members of the school community from harm to themselves or to their property
- Deter criminality in the school
- Protect school assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise during disciplinary and grievance proceedings
- To assist in the defense of any litigation proceedings
- To assist in managing the school

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency incident occurring

- Pursue any other purposes than the ones stated above

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

2. Relevant legislation and guidance

This policy is based on:

2.1 Legislation

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

2.2 Guidance

- Surveillance Camera Code of Practice (2021)

3. Definitions

Surveillance: the act of watching a person or a place

CCTV: closed circuit television; video cameras used for surveillance

Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

4. Covert surveillance

Schools within the Redhill Academy Trust will not engage in covert surveillance unless an issue is serious enough to justify it and authorised by The Headteacher and Trust Data Protection Officer. Any covert monitoring must cease once an investigation is concluded.

5. Location of the cameras (See Appendix 1)

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).

Cameras are located in:

1. Carpark facing school gates
2. Carpark facing back of school
3. KS1 external area overview
4. KS2 External area overview
5. Front entrance External Overview
6. Early Years External Overview
7. Field Overview
8. Front Entrance Internal Overview
9. Main Hall Overview

Wherever cameras are installed appropriate signage is in place to warn members of the school community that they are under surveillance. The signage:

- Identifies the school as the operator of the CCTV system
- Identifies the school as the data controller
- Provides contact details for the school

Cameras are not and will not be aimed off school grounds into public spaces or people's private property.

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

6. Roles and responsibilities

6.1 The Local Academy Board

The Local Academy Board has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

6.2 The Headteacher

The headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system

- Liaise with the Trust Data Protection Officer (DPO) and in school Data Protection Lead (DPL) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified
- Ensure that the guidance set out in this policy is followed by all staff, including the noting of all access to footage on the CCTV access log
- Review the CCTV policy to check that the school is compliant with legislation
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training in the use of the system and in data protection
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and considered the result of a data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties

6.3 The Data Protection Lead

The Data Protection Lead (DPL) will:

- Ensure that persons with authorisation to access the CCTV are trained to use the CCTV system and also trained in data protection
- Train all staff to recognise a subject access request
- Deal with subject access requests in line with the Freedom of Information Act (2000)
- Support in conducting data protection impact assessments
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed when it falls out of the retention period
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- Carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period, including the monitoring of the CCTV Access Log, ensuring that any footage downloaded and stored securely, is deleted as soon as it is no longer required.
- Receive and consider requests for third-party access to CCTV footage

6.4 The Data Protection Officer

The Data Protection Officer (DPO) will:

- Support the DPL with the tasks listed in section 6.3 above
- Monitor compliance with UK data protection law
- Act as a point of contact for communications from the Information Commissioner's Office

6.4 The System Manager

The System Manager will:

- Take care of the day-to-day maintenance and operation of the CCTV system
- Oversee the security of the CCTV system and footage
- Check the system for faults and security flaws termly
- Ensure the data and time stamps are accurate termly
- Carry out termly checks to ensure that cameras are reset to their original positions.

7. Operation of the CCTV system

The CCTV system will be operational 24 hours a day, 365 days a year.

The system is registered with the Information Commissioner's Office.

Audio recording may operate in appropriate situations e.g., reception or higher risk areas. Where this is the case, additional signage will be provided and documented in Section 5 of this policy. We will carry out an additional Privacy Impact Assessment where this applies.

Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

8. Storage of CCTV footage

Footage will be retained for 47 days. At the end of the retention period, the files will be overwritten automatically.

On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

Recordings will be downloaded and encrypted or stored in a file with limited access, so that the data will be secure and its integrity maintained, with it being available for use as evidence if required.

All recordings which are downloaded and stored must be documented the Academy CCTV log sheet, so that it's period of retention may be monitored to ensure that the recording is not retained any longer than necessary.

The DPL will carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period, including the monitoring of the CCTV Access Log, ensuring that any footage downloaded and stored securely, is deleted as soon as it is no longer required.

9. Access to CCTV footage

Access will only be given to authorised persons (see section 9.1 below), for the purpose of pursuing the aims stated in section 1.1, or if there is a lawful reason to access the footage. Any requests to view footage which does not meet these criteria must be refused.

Anyone not listed in section 9.1 wishing to have access to CCTV footage, must obtain prior authorisation from a staff member who is listed in the staff access section below. The details of **ALL** access to CCTV footage must be recorded on the CCTV access log, clearly noting the lawful reason for access and specific footage requested. Details such as the requesters name, the date and time, the reason for access and whether any footage has been downloaded and where stored, must also be

recorded. Access requested for non-school management reasons i.e. for a SAR; following a request from the Police; to support a complaint or when a personal request is received i.e. re damage to a car in the car park must always be recorded on the log in detail.

Any visual display monitors will be positioned so that only authorised personnel will be able to see the footage.

9.1 Staff access

The following members of staff have authorisation to access the CCTV footage and can authorise searches on behalf of other staff :

- The Headteacher [Emma Levers]
- The Assistant Headteachers [Joel Beeden, Dionne Daysh]
- The Data Protection Lead [Sarah Walker]
- The System/Network Manager [Craig Dudley] **(Cannot authorise searches/access by other staff members or third parties)**
- Anyone with express permission of the headteacher [Deborah Parnham]

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

All members of staff who have access will undergo training to ensure proper handling of the system and footage, and be aware of the need to record all access to footage on the CCTV Access Log.

Any member of staff who misuses the surveillance system may be committing a criminal offence and may face disciplinary action.

9.2 Subject access requests (SAR)

According to UK GDPR and DPA 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Upon receiving the request, the Data Protection Lead in school will acknowledge receipt and will then respond within 30 days. The school reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members.

All staff have received training to recognise SARs. When a SAR is received staff should inform the DPL. When making a request, individuals should provide the school with reasonable information such as the date, time, and location the footage was taken to aid school staff in locating the footage. The DPL may make contact to obtain more detailed information where necessary.

On occasions, the school will reserve the right to refuse a SAR if, for example, the release of the footage to the subject would prejudice an ongoing investigation or may not be in the best interests of the student(s).

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead.

The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is repetitive, unfounded, or excessive.

There will be no disclosure of recorded data to third parties other than authorised personnel such as the Police. Once the footage is prepared and ready to view, the person submitting the SAR will be invited into the Academy to view the footage. Where an individual insists on receiving a copy of the footage, the Trust DPO must be consulted before any footage is released. Any footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Records will be kept that show the date of the viewing of the footage/disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

9.3 Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g., assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g., investigators).

All requests for access should be set out in writing and sent to the headteacher and the DPO/DPL and recorded on the CCTV Access log, with supporting documentation.

The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose and seek legal advice if necessary.

The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.

All disclosures will be recorded by the DPO and DPL.

10. Data protection impact assessment (DPIA)

The school follows the principle of privacy by design. Privacy is considered during every stage of the deployment of the CCTV system, including the replacement, development and upgrading.

The system is used only for the purpose of fulfilling its aims (stated in section 1.1).

When the CCTV system is replaced, developed, or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary, and proportionate.

The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the DPL in conjunction with Craig Dudley

Those whose privacy is most likely to be affected, including the school community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

A new DPIA will be done annually or whenever cameras are moved, or new cameras are installed.

If any security risks are identified during the DPIA, the school will address them as soon as possible.

11. Security

- The System/Network Manager will be responsible for overseeing the security of the CCTV system and footage
- The system will be checked for faults once a term
- Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure
- Footage will be stored securely and encrypted wherever possible

- The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use
- Proper cyber security measures will be put in place to protect the footage from cyber attacks
- Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible

12. Complaints

Complaints should be directed to the Headteacher or the DPO and should be made according to the school's complaints policy.

13. Monitoring

The policy will be reviewed annually by the DPO to consider whether the continued use of a surveillance camera remains necessary, proportionate, and effective in meeting its stated purposes.

14. Links to other policies

- Data protection policy
- Privacy notices for parents, pupils, staff, governors, and suppliers
- Safeguarding policy
- Data Management Policy & Retention Schedule.