



# Rosslyn Park Primary and Nursery School CCTV Policy

Policy Number	Author	Publication Date	Review Cycle
007a	COO	V2 September 2022	Every 2 years

## Closed Circuit Television (CCTV) Policy

At our school we take our responsibility towards the safety of staff, visitors (including visiting children and property) very seriously. 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.

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 in the course of disciplinary and grievance proceedings.
- To assist in the defense of any litigation proceedings.

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 event that the Police request to view CCTV to assist in the investigation of a specific crime, this will only be provided for the specific incident and will not be released until written authority has been provided. In the unlikely event where the Police request that CCTV footage, be released to the media, again this 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.

### Relevant legislation and guidance

This policy is based on:

#### 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](#)

#### Guidance

- [Surveillance Camera Code of Practice \(2021\)](#)

#### Definitions

**Surveillance:** monitoring of school property and the movements and behaviour of individuals. For the purposes of this policy only video footage will be applicable.

**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.

#### Covert surveillance

We do not condone the use of covert surveillance when monitoring school staff or any of its visitors. Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed (such as following Police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with Data Protection law.

Any overt surveillance footage will be clearly signposted around the school.

## Purpose and justification

The school will only use CCTV for the safety and security of the school, its staff, children and visitors. CCTV is used as a deterrent for violent behaviour and damage to the school.

If the CCTV systems are no longer required the school will deactivate them.

## Location of the cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

We have a camera installed in the main reception office which is pointed to the entrance of the school site. This camera will only be used where there is a risk to the safety of any individual or child or damage to school property. The school will notify all staff and visitors of the purpose for collecting surveillance data via its data protection Privacy notices, staff noticeboards and appropriate staff briefings.

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.

## Roles and responsibilities

### The Local Governing Body

The Local governing body has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation is complied with.

### The headteacher

The headteacher as the Data Controller for our school will:

- Take responsibility for all day-to-day leadership and management of the CCTV system and ensure that processing CCTV footage is legal and fair.

- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed, justified and not excessive in relation to the reason for its collection.
- Ensure that the guidance set out in this policy is followed by all staff.
- 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 from the DPO 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 taken into account 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.
- Take measures to protect footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

**The role of the data protection officer (DPO) includes:**

- Ensure the school provides appropriate training for persons with authorisation to access the CCTV system and footage in the use of the system and in data protection.
- Ensure the school trains all staff to recognise a subject access request.
- Deal with subject access requests in line with the Freedom of Information Act (2000).
- Monitor compliance with UK data protection law.
- Advise on and assist the school with carrying out data protection impact assessments.
- Act as a point of contact for communications from the Information Commissioner's Office.
- Conduct 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.
- Check the school ensures that 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.
- Support the school to 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.
- Check that the school ensures 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.
- Check that the school ensures that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces.
- Carry out annual review with schools to determine whether footage is being stored accurately, and being deleted after the retention period.
- Receive and consider requests for third-party access to CCTV footage.

- Ensure the school has accounted for the own level of risk related to data protection and processing performance.
- Report to the highest management level of the Trust e.g. the Trustees.
- Abide by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitor the performance of the school's data protection impact assessment (DPIA) and providing advice where requested.
- Support schools to present reports regarding data processing at the school to the Governing Body; and where requested to the Trust.

### **The CCTV 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.
- Regularly check the system for faults and security flaws. 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.
- Any 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.
- Ensure the data and time stamps are accurate on the system.

### **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.
- The system will not record audio.
- Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

### **Storage of CCTV Footage**

Footage will be retained for 30 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, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required.

### **Access to CCTV Footage**

Access will only be given to authorised persons, for the purpose of pursuing the school's aims, or if there is a lawful reason to access the footage.

Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log.

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

### **Staff Access**

The following members of staff have authorisation to access the CCTV footage:

- The headteacher: Scott Mason
- The deputy head: Matt Barnham
- The data protection officer – Mrs Jill Wilkinson:
- The system manager: Andy Mullahy
- Anyone with express permission of the headteacher

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.

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

### **Subject access requests (SAR)**

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

Upon receiving the request, the school will immediately acknowledge this and offer the individual to view the recording once they have confirmed the date and time which will be within 30 days. Should the individual wish to have a copy, this will then be provided with the timescale. 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 DPO immediately. 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.

On occasion 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.

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 before viewing by the individual is undertaken. If the individual has requested a copy of the recording, and it is not possible to obscure unwarranted identification, then 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.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

The school will make arrangements for the individual to view a recording at a mutual date and time. However, should a copy be required then the school will provide this on a secure device and may charge the individual for the device needed for the copy.

Records will be kept that show the date of the 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](#).

### **Third-Party Access**

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in the aims of the policy, 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.

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.

### **Data protection impact assessment (DPIA)**

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

The system is used only for the purpose of fulfilling its aims in this policy.

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.

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.

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

### **Security**

- The system manager will be responsible for overseeing the security of the CCTV system and footage.
- The system will be regularly checked for faults.
- 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.

### **Complaints**

Complaints should be directed to the Headteacher and should be made according to the Trust's complaints policy.

### **Monitoring and Review of the Policy**

This Policy may be amended at any time to take account of changes in legislation. The normal cycle of review for this policy will be two years.