



## The Wren CCTV Policy

### Contents:

1. Aims .....	2
1.1. Statement of Intent .....	2
2. Relevant Legislation and Guidance .....	2
2.1. Legislation .....	2
2.2. Guidance .....	3
3. Definitions .....	3
4. Location of the Cameras .....	3
4.1 External.....	3
4.2 Internal.....	3
5. Roles and Responsibilities.....	4
5.1 Excalibur Trust .....	4
5.2 The Principal.....	4
5.3 The School Data Protection Officer (with support from the Trust DPO).....	4
5.4 The Site Operations Manager .....	4
6. Operation of the CCTV System.....	5
7. Storage of CCTV Footage .....	5
8. Access to CCTV Footage.....	5
8.1 Staff Access .....	6
8.2 Subject Access Requests (SAR) .....	6
8.3 Third-Party Access .....	6
9. Data Protection Impact Assessment (DPIA) .....	6
10. Security/Access.....	7
11. Complaints .....	7
12. Monitoring.....	7
13. Links to other Policies .....	7
14. Appendix A – CCTV – Staff Guidance .....	8

## 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 in the course of disciplinary and grievance proceedings

To assist in the defence 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 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.

## 4. Location of the Cameras

### 4.1 External

There are 31 cameras that cover the outside and the perimeter of the school buildings.

### 4.2 Internal

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, at the time of writing, in:

Ground floor corridors	4
First floor corridors	7
Second floor corridors	6
Staircore 1 entrance	5
Staircore 2 including entrance and lift lobby	6
Staircore 3	3
Staircore 4	3
Restaurant	3
Inclusion corridor	1
Inclusion classroom	1
Refocus Room	1
Roundhouse	1
Sports Building and Corridors	5

Appropriate signage is in place to warn members of the school community that they are under surveillance at each entrance to the school. 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.

## 5. Roles and Responsibilities

### 5.1 Excalibur Trust

The Trust 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.

### 5.2 The Principal

#### **The Principal will:**

- Take responsibility for all day-to-day leadership and management of the CCTV system
- 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 and justified
- 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 permission 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
- Provide training and guidance on appropriate live monitoring, the avoidance of excessive surveillance, and staff responsibilities when working in areas where live CCTV screens are visible.

### 5.3 The School Data Protection Officer (with support from the Trust DPO)

#### **The school Data Protection Officer (DPO) will:**

- Arrange regular training for all staff to recognise a Subject Access Request
- Deal with Subject Access Requests in line with the Freedom of Information Act (2000)
- 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
- 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
- Receive and consider requests for third-party access to CCTV footage

### 5.4 The Site Operations Manager

#### **The Site Operations 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
- Liaise with the school IT Contractor on identified faults

## 6. 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.

Live CCTV images may be monitored **for defined security, safeguarding and site-management purposes**, including:

- Monitoring access points and perimeter security
- Responding to alarms, intercom calls, or incidents
- Managing site safety during the school day
- Supporting safeguarding where there is an immediate concern
- Live monitoring will not be carried out on a routine or casual basis without a legitimate purpose.

## 7. 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 the Principal or a law enforcement body is investigating an incident, 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.

## 8. Access to CCTV Footage

### Who can view CCTV:

#### CCTV Live:

- The Principal can watch live CCTV for security and can use CCTV to observe footage involving anyone that is on site at The Wren.
- The Principal can delegate responsibility for a member of staff to watch live CCTV for security and safety reasons.
- The Site Operations Manager (Principal to delegate if absent) can view live CCTV to ensure the site is secure.

#### CCTV Footage:

- The Principal has delegated responsibility to all Senior Leadership Team (SLT) members to observe footage involving **students only** and to write a CCTV transcript without seeking permission.
- When a case arises with students only, the Principal has delegated responsibility to the Vice Principals and Assistant Vice Principal in charge of Attitudes, to grant permission for the relevant Progress Leader to view the footage and to write a CCTV transcript.
- When a case arises with staff and / or a visitor, the Principal must either observe the footage or delegate the task to a member of SLT.

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, 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 CCTV Access Log.

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

## See Appendix A

### 8.1 Staff Access

CCTV footage will only be accessed via work devices, or from the visual display monitors. Any member of staff who misuses the surveillance system may be committing a criminal offence and will face disciplinary action.

### 8.2 Subject Access Requests (SAR)

Individuals have a right to make a 'Subject Access Request' to gain access to personal information that the school or Trust holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with?
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally
- Subject access requests may be submitted in writing or verbally, either to the Trust DPO. If staff receive a subject access request, they must immediately forward it to their school Data Protection Lead, who will contact the DPO.

[“Cited Excalibur Trust Data Protection Policy”](#)

### 8.3 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.
- 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.

## 9. 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 (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.
- 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 whenever cameras are moved, or new cameras are installed.
- If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

## 10. Security/Access

- The Site Manager will be responsible for overseeing the security of the CCTV system and footage
- 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
- 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

Live CCTV screens are positioned so that footage can only be viewed by authorised staff.

Staff working in areas with live screens must be trained in appropriate use and understand that footage must not be discussed, shared, or observed without a legitimate purpose and following the school procedures.

## 11. Complaints

Complaints should be directed via the Trust complaints procedure: [Concerns & Complaints - Excalibur Academies Trust](#)

## 12. 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.

## 13. Links to other Policies

- [Data protection policy](#)
- [Privacy notices for parents, students, staff, governors and suppliers](#)
- [Safeguarding policy](#)

## 14. Appendix A – CCTV – Staff Guidance

**Applies to:** All staff who work in areas where live CCTV screens are visible or who may be authorised to view CCTV.

### Purpose of this guidance

This guidance explains how live CCTV must be viewed and used at the school. It supports the school's CCTV Policy and ensures compliance with data protection law while maintaining effective safeguarding and site security.

### Why the school uses live CCTV

Live CCTV is used **only for legitimate purposes**, including:

- Safeguarding students, staff and visitors
- Monitoring access points, gates and perimeter security
- Responding to incidents, alarms or intercom calls
- Supporting site safety and security during the school day

CCTV is **not** used for general supervision, performance management, or to monitor individuals without cause.

### Live screens in the site office

- Live CCTV screens may be displayed continuously in the site office or other secure areas.
- The presence of live screens supports **situational awareness** and allows a prompt response if a concern arises.
- Staff are **not expected to actively watch screens at all times.**

This means:

- Screens may be visible
- Active monitoring should only take place when there is a **specific reason**

### Who can access CCTV – live and recorded

#### Live CCTV (real-time viewing)

Live CCTV may only be viewed by the following authorised roles:

- The Principal
- Members of the Senior Leadership Team (SLT) when delegated by the Principal
- The Site Operations Manager (or delegated site staff when authorised by the Principal)

Authorised staff may view live CCTV **only for legitimate security, safeguarding, or site-management purposes.**

Live CCTV may be actively observed when:

- An incident has been reported or is suspected
- An alarm or intercom has been activated
- There is a safeguarding or welfare concern
- Site security checks are required (e.g. gates, perimeter)
- The Principal or a delegated senior leader has directed the viewing

Staff who are not authorised must not view live CCTV, even if screens are visible.

## Recorded CCTV footage

Access to recorded CCTV footage is **more restricted** than live viewing.

Recorded footage may only be accessed by:

- The Principal
- Members of SLT acting under delegated authority

Specific permissions:

- **Student-only incidents:** SLT may view footage and produce CCTV transcripts in line with the CCTV Policy. Progress Leaders may only view footage with SLT approval.
- **Incidents involving staff or visitors:** Footage must be viewed by the Principal or a delegated SLT member.

All access to recorded footage must:

- Be for a lawful and legitimate purpose
- Be logged in the CCTV Access Log
- Comply fully with the school's CCTV Policy and data protection law

Always ensure your access has a **clear and recorded purpose**.

## What is NOT acceptable

You must not:

- Watch CCTV out of curiosity or habit
- Track or follow individuals without a legitimate reason
- Use CCTV to monitor staff performance
- Discuss CCTV footage with unauthorised persons
- Allow unauthorised individuals to view live screens

Misuse of CCTV may result in disciplinary action and could constitute a criminal offence.

## Privacy and professionalism

- Be mindful that CCTV footage is personal data.
- Do not comment on or share what you see unless it is necessary and appropriate.
- If you are unsure whether viewing is appropriate, **do not proceed** and seek advice.

## Access to recorded footage

- Viewing recorded CCTV footage is **more restricted** than live viewing.
- Only authorised staff may access recordings, and this must be logged.
- Permission must be obtained in line with the CCTV Policy.

## If you are unsure

If you are uncertain about:

- Whether you should view live CCTV
- Whether something you have seen should be acted upon
- How CCTV footage may be used or shared

Speak to the **Principal, Site Operations Manager, or Data Protection Officer (DPO)**.

**Remember:** CCTV is there to keep everyone safe. It must always be used lawfully, proportionately and respectfully.

### Staff acknowledgement and declaration

I confirm that:

- I have read and understood Appendix A Staff Guidance.
- I understand who is authorised to view live CCTV and recorded footage.
- I understand that CCTV must only be accessed for legitimate security, safeguarding or site-management purposes.
- I understand that misuse of CCTV may result in disciplinary action and could constitute a criminal offence.
- I agree to comply fully with the school's CCTV Policy and data protection requirements at all times.

**Name:** \_\_\_\_\_

**Role:** \_\_\_\_\_

**Signature:** \_\_\_\_\_

**Date:** \_\_\_\_\_