CCTV POLICY

Date of Review: June 2025

Reviewed by: Mrs R Fawcett, Operations Manager & School Data Protection Lead and Mrs K Long, ICT Team Leader

Approved by Governors: June 2025

Frequency of Review: Annually

Date of Next Review. September 2026

Contents

1. Aims

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

The system comprises a number of fixed-based and Pan-Tilt-Zoom cameras located around the school site. All cameras are monitored via access to secure servers and only available to authorised users.

1.1 Statement of intent

At President Kennedy School, we take our responsibility towards the safety of our students, staff and visitors very seriously. To this end, we use surveillance cameras to monitor any instance of physical aggression or physical damage to our school and its members, and to monitor any unauthorised access to our site.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV system at the school and ensure that:

- We comply with all relevant Data Protection legislation, including UK General Data Protection Regulation and the Data Protection Act 2018
- The images that are captured are useable for the purposes we require them for
- We reassure those persons whose images are being captured that the images are being handled in accordance with data protection legislation

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- To enhance the safety and security of students, staff and visitors to the school site
- To monitor and improve student behaviour and reduce internal truancy
- To monitor in real time/track suspicious persons/activity
- To investigate allegations of poor student behaviour or other members of the school community (including parents/carers) or allegations against staff, where it is necessary and proportionate to do so
- To provide evidence for insurance claims where it is necessary for the quick and efficient processing of claims
- To protect school property from criminal activity such as vandalism, graffiti and other environmental crime
- To deter criminals from conducting criminal activity on our premises
- To assist police to deter and detect crime

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 suspicious or 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's Office under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and the 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 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

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.

5. Location of the cameras

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 both internal and external areas around the school premises.

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

With the exception of the area in the vicinity of the school gate, cameras are not and will not be aimed off school grounds into public spaces or people's private property.

Our cameras are located in areas where staff and students have access. They are not located in sensitive areas where privacy is expected, e.g. changing rooms or toilet cubicles. Some cameras are be located in the corridor areas near the open-plan toilet areas and changing rooms – the cameras cannot see into cubicles which also have their privacy protected by floor to ceiling doors.

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

The CCTV system does not record audio.

5.1 Sky Blues in the Community

The Sky Blues in the Community lease a pavilion building and the 3G pitch from President Kennedy School. They have installed a number of CCTV cameras around this building and sports facility. For these cameras and CCTV system, they operate as the Data Controller and are responsible for its maintenance and operations.

Sky Blues in the Community will conduct their own Data Protection Impact Assessment (DPIA) on the CCTV system and have their CCTV Policy.

The Sky Blues in the Community will provide CCTV access to designated members of the President Kennedy School staff upon request for the purposes of accident and incident investigation and site security and operations.

6. Roles and responsibilities

6.1 The Local Governing Committee

The Local Governing Committee (LGC) 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 role of the headteacher is to:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the 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
- 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 DPL and ICT Team Leader and having taken into account the result of a DPIA
- Decide, in consultation with the DPL and Designated Safeguarding Lead, whether to comply with disclosure of footage requests from third parties

6.3 The Data Protection Lead (DPL)

The DPL will:

- Ensure staff with authorisation to access the CCTV system and footage receive training in the use of the system and in data protection
- Train all staff to recognise a Subject Access Request (SAR)
- Deal with SARs in line with the UK GDPR and Data Protection Act 2018
- Monitor compliance with UK data protection law
- Conducting a data protection impact assessment on the CCTV system
- Act as a point of contact for communications from the Information Commissioner's Office (ICO)
- 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 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
- Receive and consider requests for third-party access to CCTV footage

6.4 The ICT Team Leader

The ICT Team Leader 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
- 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

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.

The system will not record audio.

Recordings will have date and time stamps. This will be checked by the ICT Team Leader termly and when the clocks change.

8. Storage of CCTV footage

Images are stored on the hard drive of the Network Attached Storage Device (NAS), which are housed within the school's main server room. Images are retained for 30 rolling days unless requested as part of an incident and then stored on archive for 12 months.

The data management system will automatically delete the data after 30 days. If images are required as part of an incident or investigation, they will then be archived on SharePoint for 12 months.

9. Access to CCTV footage

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.

A record must be held of any external and third-party individuals that access the footage and must note their name, the date and time, and the reason for accessing the access log.

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

9.1 Staff access

Only authorised personnel who are employed to work within the ICT team have full operational access to the CCTV system, including the moving cameras. They are:

- Kirsty Long – ICT Team Leader
- Jack Stanley – ICT Technician
- Dave Barrett – ICT Technician

Members of the Admin team have limited live access to CCTV footage of individuals (predominantly students) entering/exiting at the Student Reception gate. This is for the purpose of safeguarding – only allowing access/egress to known individuals (students).

Access to the CCTV system is restricted to the ICT team. They are able to view images on any computer throughout the school, however their login to the school computer system is password protected and then access to the CCTV system is also password protected.

Data may be shared by the ICT team with anyone with the express permission by the Headteacher or Head or School. This will predominantly be:

- The school's Safeguarding Leads
- SLT
- Facilities Manager
- School Data Protection Lead
- College teams

The school's CCTV support contractor, Active Communications also have access to the CCTV system in order to be able to maintain and upgrade it as and when needed.

CCTV footage will only be accessed from authorised staff's work devices.

All members of staff who have access will undergo training to ensure proper handling of the system and footage.

Any member of staff who misuse the surveillance system may be committing a criminal offence, and may be subject to disciplinary action.

9.2 Subject access requests (SARs)

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

All requests should be made in writing to the Data Protection Lead, Mrs Rebecca Fawcett who can be contacted by email at Fawcettr@pks.coventry.sch.uk. 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.

All staff have received training to recognise SARs. When a SAR is received staff should immediately inform the DPL in writing.

Upon receiving SAR, the school will immediately issue an acknowledgment of the request and will then respond within 1 calendar month. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within 1 month of the receipt of the request.

On occasion the school will reserve the right to apply exemptions and refuse to comply with a SAR and/or refuse access to CCTV. Examples of when this may happen include if the release of the footage to the subject would prejudice the rights of other individuals or jeopardise 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. 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 a 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 does not have a facility to provide copies of CCTV footage but instead the applicant may view the CCTV footage if available.

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.

9.3 Access and disclosure to third parties

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 communicated to the Headteacher, the school Safeguarding team or the DPL.

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 Head teacher and DPL will consider very carefully how much footage to disclose, and seek legal advice if necessary.

The Headteacher and DPL will ensure that any disclosures that are made are done in compliance with the UK GDPR.

All disclosures will be recorded by the DPL.

10. 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 DPL will carry out the DPIA.

A new DPIA will be done every two years and/or whenever cameras are moved, and/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.

11. Security

The ICT Team Leader 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

Robust 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 and should be made according to the Trust's Complaints Policy.

13. Monitoring

The policy will be reviewed annually by the DPL 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

This CCTV policy has links to other Trust or school policies as follows:

- TFT Data Protection Policy
- Privacy Notices for Parents/Carers and students, Staff, Governors, Visitors and Applicants
- Security Policy
- Child Protection and Safeguarding Policy