CCTV Policy

Author	David Marchant
Agreed by	Trust Board
Date agreed	March 2023
Date to be reviewed	March 2024

CONTENTS

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.

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/investigate incidents
- 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 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.

RELEVANT LIGISLATION 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: 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

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, the proper authorisation forms from the Home Office will be completed and retained.

LOCATION OF THE CAMERAS

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system

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

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 TRUST BOARD

The trust 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.

THE HEADTEACHER

The headteacher 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 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

THE DATA PROTECTION OFFICER

The data protection officer (DPO) will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system and 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)
- 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
- 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
- Receive and consider requests for third-party access to CCTV footage

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

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.

The DPO will carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period.

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.

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

- The site manager
- The data protection officer
- The system manager
- Anyone with express permission of the headteacher

CCTV footage will only be accessed from authorised personnel's 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 DPA 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of section 9 of the Trust's Data Protection Policy. The school reserves the right to charge for this.

When such a request is made, the DPO or their appropriately nominated representative will review the CCTV footage, in accordance with the request.

If the footage contains only the individual making the request, then that individual may be permitted to view the footage. This must be strictly limited to that footage which contains only the images of the individual making the request. The Head of Premises and Estates or their representative must take appropriate measures to ensure that the footage is restricted in this way.

If the footage contains images of other individuals, then the Trust must consider whether

• The request requires the disclosure of the images of individuals other than the requester, for example, whether the images can be distorted so as not to identify the individuals.

• The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained;

• If not, then whether it is otherwise reasonable, in the circumstances, to disclose those images to the individual making the request.

The DPO must record and keep securely records of all disclosures, which sets out

• When the request was made.

• The process followed in determining whether the images contained third parties.

• The considerations as to whether to allow access to these images.

• The individuals that were permitted to view the images and when.

• Whether a copy of the images was provided and, if so, to whom, when and in what format.

All such requests shall be assessed in conjunction with the Trust's Freedom of Information and Data Protection Policies by the Trust Data Protection Officer.

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 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 or 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 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 DPO and the Headteacher.

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 when this policy is renewed i.e. at least annually, when 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.

SECURITY

- The system 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

COMPLAINTS

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

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.

LINKS TO OTHER POLICIES

- Data protection policy
- Privacy notices for parents, pupils, staff, governors and suppliers
- Safeguarding policy

APPENDIX 1 - CHECKLIST

This CCTV system and the images produced by it are controlled by the Headteacher who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose.

QEGS has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of students, staff and visitors. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

	Checked (Date)	Checked (By)	Date of Next Review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.	1/3/23	Headteacher	1/3/23
There is a named individual who is responsible for the operation of the system.	1/3/23	Headteacher	1/03/24 or before if required
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.	1/3/23	Headteacher	1/03/24 or before if required
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.	1/3/23	Headteacher	1/03/24 or before if required
Cameras have been sited so that they provide clear images.	1/3/23	Headteacher	1/03/24 or before if required
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.	1/3/23	Headteacher	1/03/24 or before if required
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).	1/3/23	Headteacher	1/03/24 or before if required
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	1/3/23	Headteacher	1/03/24 or before if required
The recorded images will only be retained long enough for any	1/3/23	Headteacher	1/03/24 or before if required

incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.	1/3/23	Headteacher	1/03/24 or before if required
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.	1/3/23	Headteacher	1/03/24 or before if required
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.	1/3/23	Headteacher	1/03/24 or before if required
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	1/3/23	Headteacher	1/03/24 or before if required

APPENDIX 2 – DATA PROTECTION IMPACT ASSESMENT

1	Site details.
	QEGS Penrith Inc. Sixth Form block
2	Who will be captured on CCTV?
	Students / Staff / Visitors / Public
3	What personal data will be processed?
	Images
4	Why is the camera / system being installed? What is the issue that the Trust is trying to address? Is CCTV the best solution?
	Safety, welfare and security of Staff/Students/Visitors/School Buildings & Assets
5	What is the lawful basis for operating the CCTV system?
	Legal obligation, legitimate interests of the organisation to maintain health and safety and to prevent crime.
6	Who is/are the named person(s) responsible for the system?
	Headteacher

7	Describe the CCTV System.
	The site has cameras located within the grounds externally, with plans for internal cameras in key locations. The cameras are high specification, fixed lens type with no sound recording ability, so that the images can be used for the purpose intended. Cameras have been situated in order to avoid capturing images which are not necessary. Signs indicating that CCTV is in operation are located at various places around the sites.
8	Set out the details of any sharing with third parties.
	CCTV footage may be provided to external parties such as the Police or through subject access requests. All recorded data is stored locally on internal hard drives.
9	Set out the retention period of any recordings
	No longer than required for purpose to a maximum of 30 days unless there is legitimate reason to retain specific recordings.
10	Set out the security measures in place to ensure that recordings are captured and stored securely.
	CCTV footage is only accessible by authorised personnel and this access is password protected. The footage is stored is stored locally on internal hard drives.
11	What are the risks to the rights and freedoms of individuals who may be captured on the CCTV footage?
	1. Identification of an individual. 2. Loss of data, if recordings are disclosed to a third party and not encrypted. 3. Misuse of data if accessed by unauthorised individual.

12	What measures are in place to address the risks identified?
	1. Identification will only be sought for justifiable reasons and by authorised personnel. 2. Data to be downloaded to a BitLocker encrypted USB stick or other secure transfer mechanism. 3. Authorised users are required to sign in using their personal login.
13	Have parents and pupils been consulted where appropriate, as to the use of the CCTV system?
	Yes – through policies and data privacy notices.
14	When will this P.I.A. be reviewed?
	As required, or with any changes to the CCTV system(s) in use but in any event at least annually as part of the review of this policy.