CCTV Policy

Park Community School

Contents

Introduction 3
Purpose of policy 3
Scope 3
General Principles 3
Justification for use of CCTV 4
Location of Cameras 4
Covert Surveillance 5
Notification - Signage 5
Storage and Retention 5
Access 6
Responsibilities 7
Implementation and Review 8
Appendix 1 - Definitions 9
Appendix 2 - The General Data Protection Regulations 2018: data protection principles 10
Appendix 3 - The guiding principles of the Surveillance Camera Code of Practice Information Commissioner's Office (ICO) 11

Introduction

Closed Circuit Television Systems (CCTVS) are installed in Park Community School. Any new CCTV systems will be introduced in consultation with the Headteacher, Head of School, Co-Chairs of Governors and Facilities Manager and Bursar. Systems already in operation, will be reviewed regularly by the above.

Purpose of policy

The purpose of this policy is to regulate the use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external environs of the premises under the remit of Park Community School and its associated premises.

CCTV systems are installed (both internally and externally) for the purpose of enhancing security of the buildings, associated equipment and safety of occupants. The surveillance security system is in operation within and or in the external environs of the premises 24 hours a day. CCTV surveillance at Park Community School and associated premises is intended for the purposes of:

- Protecting the school buildings and school assets, at all times;
- Promoting the health and safety of staff, students and visitors;
- Preventing bullying;
- Reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- Supporting the Police in a bid to deter and detect crime;
- Assisting in identifying, apprehending and prosecuting offenders;
- Ensuring that the school rules are adhered to.

Scope

This policy relates directly to the location and use of CCTV and monitoring, recording and subsequent use of such recorded material. Where classes and activities are carried out in rented premises, Park Community School will ensure the CCTV systems, where installed, are operated in a way that is compatible with the provisions of this policy.

General Principles

Park Community School as the corporate body has a statutory responsibility for the protection of its property and equipment as well as providing a sense of security to its employees, students and invitees to its premises. Park Community School owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation CCTV systems, associated monitoring and recording equipment are used as an added mode of security and surveillance.

The use of the CCTV system will be conducted in a professional, ethical and legal manner. Use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.

Information obtained through the CCTV system may only be released when authorised by the Headteacher or a designated manager. Any requests for CCTV recordings/images by the police will be fully recorded and legal advice will be sought if any such request is made. (See "Access" below).

CCTV monitoring of public areas will be conducted in a manner consistent with all existing policies adopted by the school, including Equality Policy and the Dignity at Work Policy.

Video monitoring of public areas for security purposes within the school premises is limited to use that does not violate the individual's reasonable expectation to privacy.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the school. All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the school. Recognisable images captured by CCTV systems are "personal data." They are therefore subject to the provisions of the General Data Protection Regulations 2018 (GDPR).

Justification for use of CCTV
The GDPR 2018 principles requires that data is processed lawfully, fairly and transparently, collected for a specific purpose and relevant and necessary for that specific purpose. It also requires that data is not kept longer than necessary and is kept secure and protected.

CCTV systems will not be used to monitor normal teacher/student classroom activity in school.

In other areas of the school where CCTV has been installed, e.g. hallways, stairwells, locker areas, the Headteacher has demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that have arisen prior to the installation of the system.

Location of Cameras
The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. Park Community School has endeavoured to select locations for the installation of CCTCV cameras which are least intrusive to protect the privacy of individuals. Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

CCTV Video Monitoring and Recording of Public Areas at Park Community and associated premises will include the following:

- **Protection of school buildings and property:** The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services
- **Monitoring of Access Control Systems:** Monitor and record restricted access areas at entrances to buildings and other areas
- **Verification of Security Alarms:** Intrusion alarms, exit door controls, external alarms

- **Video Patrol of Public Areas:** Parking areas, Main entrance/exit gates, Traffic Control
- **Criminal Investigations (carried out by Police):** Robbery, burglary, assault and theft surveillance

Covert Surveillance
Park Community will only install covert surveillance cameras under the direction of the Headteacher or Head of School once agreed by the Co-Chairs of Governors. These will be installed out of hours under the guidance of the Facilities Manager, linking the cameras to only his PC.

Notification - Signage
The CCTV Policy will be available for all on the website. Adequate signage will be placed around the site indicating that CCTV is in operation, at Park Community School and associated premises. An example of signage is given below; the actual signs may vary.

WARNING
CCTV cameras in operation
Images are being monitored and recorded for the purpose of crime-prevention, the prevention of anti-social behaviour, the prevention of bullying, for the safety of our staff and students and for the protection of Park Community School and its property. This system will be in operation 24 hours a day, every day. These images may be passed to Police.

Appropriate locations for signage include:
- at entrances to premises i.e. external doors, school gates
- reception area
- at or close to each internal camera

However, signs will not be located at all doors or at all camera points.

Storage and Retention
Section 2(1)(c)(iv) of the General Data Protection Regulations 2018 states that data "shall not be kept for longer than is necessary for" the purposes for which it was obtained. The normal length of retention will be 30 days.

The images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher but may delegate the administration of the CCTV System to another staff member. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

CCTV will be stored securely on the schools "One drive" with restricted access. Access will be restricted to authorised personnel only. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

Access
Access to the CCTV system and stored images will be restricted to authorised personnel only i.e. Headteacher, Head of School or the designated manager.

In relevant circumstances, CCTV footage may be accessed:

- By Police where the school are required by law to make a report regarding of a suspected crime
- Following a request by Police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on the school site or associated premises
- To the HSE and/or any other statutory body charged with child safeguarding;
- To assist the Headteacher, Head of School or designated manager in establishing facts in cases of unacceptable student behaviour (see Behaviour Policy)
- By individuals (or their legal representatives) subject to a court order.
- To the school insurance company for evidence regarding damage done to the insured property.

Requests by Police: Information obtained through CCTV monitoring will only be released when authorised by the Headteacher, Head of School or designated manager. If Police request CCTV images for a specific investigation, Police may require a warrant and accordingly any such request made by Police should be made in writing and the school should seek legal advice.

Subject Access requests: On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, unless an exemption/prohibition does not allow to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. To exercise their right of access, a data subject must make an application in writing to the school's Data Protection Officer, including relevant court order where applicable.

Access requests can be made to the following: Data Protection Officer, Park Community School, Middle Park Way, Havant, Hampshire PO9 4BU.

A person should provide all the necessary information to assist the school in locating

the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the school.

Recorded images are not routinely kept for more than 30 days.

In giving a person a copy of their data, the school may provide a still/series of still pictures, a disk or memory stick with relevant images. However, other images of other individuals will be redacted.

We will not release information/images, however, where the school believes the safeguarding of students or school security may be compromised, or where redaction is not reasonably possible. A charge may be made for the work required to find the requested images and any redactions.

Responsibilities

The Headteacher will:

- Ensure the use of CCTV systems is implemented in accordance with the policy agreed by Park Community School.
- Oversee the use of CCTV monitoring for safety and security purposes within Park Community School.
- Ensure CCTV monitoring systems will be evaluated for compliance with this policy.
- Ensure that the CCTV monitoring at Park Community or associated premises is consistent with the highest standards and protections.
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
- Maintain a record of access, e.g. an access log, to or the release of CDs or any material recorded or stored in the system.
- Ensure that recordings are not duplicated for public release.
- Approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. **Note**: temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by Police.
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that images recorded digitally are stored for a period no longer than approximately 30 days and are then erased or overwritten unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Headteacher, Head of School or Governing Body.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

- Ensure that where Police request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the Headteacher and Governing Body.
- The Headteacher may delegate responsibility to another senior member of staff.

Implementation and Review

The policy will be reviewed and updated every three years or if any changes to the law. However, should on-going review and information or guidelines, change of the policy will be updated sooner.

Once adopted by the Governing Body implementation of the policy will be monitored by the Headteacher, Head of School, or designated manager.

Document Control Table	
Associated Documents	• Equality Policy • Staff Dignity at Work Code of Conduct • Behaviour Policy
Date Approved by Governors	12/03/2025
Date of Review	March 2028

Appendix 1 - Definitions

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy

CCTV – Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on DVD or other digital recording mechanism.

The Data Protection Acts – The General Data Protection Regulations 2018 (GDPR) and Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All school staff must comply with the provisions of the GDPR when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Subject Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.

Data Processing - performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data,
- Retrieving, consulting or using the data,
- Disclosing the data by transmitting, disseminating or otherwise making it available,
- Aligning, combining, blocking, erasing or destroying the data.

Data Subject – an individual who is the subject of personal data.

Data Controller - a person who controls the contents and use of personal data i.e. the school (through the Governing Body.)

Data Processor - a person who processes personal information on behalf of the data controller but does not include an employee of the data controller who processes such data in the course of their employment i.e. a supplier or contractor who carries out work 'handling data' for the school e.g. SIMS Capita.

Appendix 2 - The General Data Protection Regulations 2018: data protection principles

1. Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

(a) "processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Appendix 3 - The guiding principles of the Surveillance Camera Code of Practice Information Commissioner's Office (ICO)
issued under the Data Protection Act 1998 (DPA) covering the use of CCTV in 2000
Version 1.2 2017-06-09

1. System operators should adopt the following 12 guiding principles:
2. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
3. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
4. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
5. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
6. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
7. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
8. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
9. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
10. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
11. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
12. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
13. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.