WANSTEAD HIGH SCHOOL

CCTV Policy

Person Responsible	Ms D Cini
Review Frequency	Every 3 years
Last Reviewed	December 2022
Next Review Date	Spring Term 2026/27
Committee	Behaviour, Attitudes & Personal Development
Ratified by Full Governing Body on	18 March 2024
This policy is communicated by the following means	School Website

Contents

Related Policies
Data Protection Policy (including SAR Appendix)
Behaviour Policy
Exclusion Policy

1. Introduction

CCTV has the potential to be privacy intrusive. The school will perform a Data Protection Impact Assessment when installing or moving CCTV cameras to consider the privacy issues involved with using new surveillance systems to ensure that the use is necessary and proportionate and address a pressing need identified.

2. Purpose of Policy

The purpose of this policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television). CCTV systems are installed in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day.

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. The school complies with the Data Protection Act and Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its use. Further details about access to the CCTV footage and images are found in the Data Protection Policy.

CCTV surveillance at the school is intended for the purposes of:

- To protect the school buildings and school assets, both during and after school hours.
- To promote the health and safety of staff, pupils and visitors as well as for monitoring pupil behaviour.
- To protect pupils, staff and visitors against harm to their person and/or property.
- To increase a sense of personal safety and reduce the fear of crime.
- To support the police in preventing and detecting crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To assist in establishing cause of accidents and/or other adverse incidents.
- To take steps to mitigate the risk of similar occurrences.
- To assist in managing the school.
- To prevent and reduce the incidence of crime, bullying and anti-social behaviour (including theft and vandalism).

Review of this policy shall be every two years and, whenever new equipment is introduced, a review will be conducted.

3. Location of Cameras

CCTV Video Monitoring and Recording of Public Areas may 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 the police): Robbery, burglary and theft surveillance.

CCTV cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities, etc.

The CCTV system is owned and operated by the school, the deployment of which is determined by the school's Senior Leadership Team. The cameras are sited so that they only capture images relevant to the purposes for which they have been installed (as described above), and care will be taken to ensure that reasonable privacy expectations are not violated. The school will ensure that the location of equipment is carefully considered to ensure that the images captured comply with the legislation. The school will make every effort to position the cameras so that their coverage is restricted to the school premises, which includes both indoor and outdoor areas.

CCTV will NOT be used in classrooms in areas in which individuals would have an expectation of privacy such as toilets, changing facilities. They will be used in areas within the school that need additional monitoring such as corridors or entrances/exits.

4. Scope

CCTV warning signs will be clearly and prominently placed at the main external entrance to the school. Signs will contain details of the purpose for using CCTV.

In areas where CCTV is used, the school will ensure that there are prominent signs placed within the controlled area. The planning and design have endeavoured to ensure that the system will give maximum effectiveness and efficiency, but it is not guaranteed that the system will cover or detect every single incident taking place in the areas of coverage.

The introduction of, or changes to, CCTV monitoring will be clearly and transparently shared with staff with an opportunity for staff to feedback. Governors will be informed of the school's decision and will have an opportunity to ask questions.

The school's CCTV is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2016/679.
All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are made aware of their responsibilities in following the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of recorded images. Access to images is currently available to:

- Donna Cini – Director of Inclusion / Designated Safeguarding Lead
- Helise Martin – Deputy Headteacher / Deputy Designated Safeguarding Lead
- Emma Hillman – Headteacher
- Eleni Bray – Deputy Headteacher
- Zeeshan Ali – Assistant Headteacher
- Mick Debono and site staff

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies and related legislation. Video monitoring of public areas for security purposes within school premises is limited to uses that do 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, or a pupil attending the school. All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the school.
CCTV monitoring will never be used in any observing or monitoring of staff unless a clear breach of the school's Code of Conduct and/or Safeguarding Policy has been observed.

Recognisable images captured by CCTV systems are 'personal data'. They are therefore subject to the provisions of the General Data Protection Regulation and Data Protection Act 2018.

Access to recorded images will be restricted to the staff authorised to view them and will not be made widely available. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. The Headteacher may delegate the administration of the CCTV System to another staff member. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis. Heads of Year and Pastoral Support Managers may be asked to view footage to assist with their investigations into pupil incidents.

5. System Management

Access to the CCTV system and data shall be password protected and will be kept in a secure area.

The CCTV system will be administered and managed by Dan Emerton, network manager who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager, the system will be managed by Haroldas Stankevicius, IT Technician.

The system and the data collected will only be available to the Systems Manager, his/her replacement and appropriate members of the senior leadership team as determined by the Headteacher.

The CCTV system is designed to be in operation 24 hours a day 7 days a week, though the school does not guarantee that it will be working during these hours.

The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that cameras are functional.

Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by proving clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those mentioned above, requests access to the CCTV data or system, the System Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists, access will be refused.

Details of all visits and visitors will be recorded in a system log book including time/data of access and details of images viewed and the purpose for so doing.

6. Downloading Media

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings), any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures:

(a) Each downloaded media must be identified by a unique mark.
(b) Before use, each downloaded media must be cleaned of any previous recording.
(c) The System Manager will register the date and time of downloaded media insertion, including its reference.
(d) Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a downloaded media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.
(e) If downloaded media is archived, the reference must be noted.
(f) If downloaded media is put onto a device, the device will be encrypted and password protected.

Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/her replacement and the Headteacher and other authorised leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable, if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the school and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The school also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media, this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the school to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until needed by the police.

Applications received from outside bodies (e.g., solicitors or parents) to view or release images will be referred to the school's Data Protection Officer and a decision made by a senior leader of the school in consultation with the school's Data Protection Officer.

7. Access to CCTV images by staff

Individuals have the right to request CCTV footage relating to themselves under the Data Protection Act and the GDPR.

All requests should be made in writing to the Data Protection Officer. Individuals submitting requests for access will be asked to provide sufficient information to enable footage relating to them to be identified. For example: time, date and location.

The applicant may view the CCTV footage if available.

The school will respond to requests within 30 days of receiving the request.

The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

8. Access to CCTV images, Subject Access Requests (SARs) and Access and Disclosure of images to Third Parties

This process is outlined in the Data Protection Policy.

9. Responsibilities

The Headteacher will:

- Ensure that the use of CCTV systems is implemented in accordance with this policy.
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the school.
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy.
- Ensure that the CCTV monitoring is consistent with the highest standards and protection
- 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 (eg. an access log) to or the release of tapes or any material recorded or stored in the system.
- Ensure that monitoring recorded tapes are not duplicated for release.
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.
- Give consideration to both pupils 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 all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place.
- 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 the NVR is only accessed and managed by authorised personnel.
- Ensure footage is not kept for longer than required. Footage is currently available for the previous 30 days which is then automatically overwritten if not required as part of a criminal investigation or court proceedings (criminal or civil). This is stored on an NVR unit in the server room with restricted access.

- On occasion footage may be retained for longer than 30 days, for example where there is:
    - an open and on-going criminal investigation;
    - a safeguarding investigation;
    - footage pertaining to a suspension or permanent exclusion to give professionals or family involved the opportunity to view the images as part the process;
    - a complaint or potential complaint received via the Complaints Policy and footage may be needed as part of the process;
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.
- Inform the Governing Body of any prospective changes to CCTV within the policy review schedule.

10. Policy Review

The Data Protection Officer is responsible for monitoring and reviewing this policy. This policy will be reviewed every two years. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

11. Complaints about the use of CCTV

Any complaints in relation to the school's CCTV system should be addressed to the Headteacher.