PLASHET SCHOOL

Working together to promote & celebrate achievement

CCTV Policy

Revised and applicable from 8th December 2023

Signed: 

Chair of Governors

Contents

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.

Statement of intent

At Plashet School, we take our responsibility towards the safety of staff, visitors and students very seriously. To that end, we use CCTV cameras to monitor any instances of aggression or physical damage to our school and its members, and to monitor any unauthorised access to our site. The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

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 or incidents
- 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 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 knowledge/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:

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)

3. Definitions

Surveillance: the act of monitoring a person or a place.

CCTV: closed circuit television; video cameras used for surveillance.

Covert surveillance: operation of cameras in the form of additional devices which are not notified 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.

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

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 internally in circulation areas and externally in staff car parks, student social areas and across the school grounds.

Wherever cameras are installed, appropriate signage is in place to warn members of the school community that they are under surveillance. As required by the code of practise of The Information Commissioner, 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.

6. Roles and responsibilities

The Governing Board

The Governing 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 Head Teacher

The Head Teacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system.
- Meet with the Premises Manager and School Business Manager to decide where CCTV is needed to justify its means.
- Liaise with the school's Data Protection Consultant 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 school's Data Protection Consultant and taken into account the result of a data protection impact assessment.
- Decide, in consultation with the school's Data Protection Consultant , whether to comply with disclosure of footage requests from third parties.

Furthermore, in consultation with the schools Data Protection Consultant, through the procurement of training resources or by the delegation of responsibility to the System Manager, the Premises Manager and School Business Manager, the Headteacher 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 School Business Manager

The School Business Manager will:

- Act as a point of contact for communications from the Information Commissioner's Office.
- Organise subject access request and data protection training for staff with access to the CCTV system or who are likely to field access requests.
- Liaise with the schools Data Protection Consultants, as required by the Headteacher, to ensure compliance with Data Protection and Freedom of Information legislation.
- Liaise with the System Manager and Premises Manager to prepare Data Protection Impact Assessments as required by this policy.

The System Manager

The System Manager will:

- Manage user accounts to the CCTV system.
- Manage internal access requests to review footage.
- Verify that footage is being stored and deleted in accordance with this policy.
- Manage receipt of Subject Access Requests sent to the Head Teacher.
- Maintain a record of all CCTV releases.
- Liaise with the School Business Manager and Premises Manager to prepare Data Protection Impact Assessments as required by this policy.

The Premises Manager

The Premises 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.
- Liaise with the system installer to ensure colleagues with system access are properly trained.
- Liaise with the School Business Manager and Systems Manager to prepare Data Protection Impact Assessments as required by this policy.

7. Operation of the CCTV system

The CCTV system will be operational 24 hours a day, 365 days a year, though the school does not guarantee that it will work during these hours.

The system is registered with the Information Commissioner’s Office.

Neither south or north site systems will record audio.

Recordings will have date and time stamps. This will be checked by the System Manager termly and when the clocks change.

8. 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.

In the absence of a compelling need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than 6 months.

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

9. Access to CCTV footage

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

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.

Internal Access and requests to view footage should follow the protocols set out in Appendix 1

Staff access

The following members of staff have authorisation to access the CCTV footage:

- The Head Teacher: Rachel McGowan
- The Deputy Head Teachers: Tomas O Donnell and Sarah Heath
- The School Business Manager: Damian Osman
- The System Manager: Zeenat Ali
- The Premises Manager: Pat Moran.
- Anyone with express permission of the Head Teacher

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

Upon receiving the request the school will issue a receipt and then respond within 30 days during term time. The school reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members.

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 one month of the receipt of the request.

Staff have received training to recognise SARs. 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.

On occasion the school will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation, if it is manifestly unfounded, manifestly excessive or if an exemption applies.

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 an 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.

We will share the files securely via download to an encrypted and password protected storage device.

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 Head Teacher.

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 will consider very carefully how much footage to disclose, and seek legal advice from the school's Data Protection Consultant as required.

The Head Teacher will liaise with the school's Data Protection Consultants to ensure that any disclosures that are made are done in compliance with UK GDPR. All disclosures will be recorded by the System Manager.

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 school's Data Protection Consultants will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the School Business Manager, System Manager and Premises Manager.

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, 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 Premises 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.
- 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.

Breaches of Security

Any breach of the Code of Practice by school staff will be initially investigated by a Deputy Head Teacher in order for the Head Teacher to take the appropriate disciplinary action.

Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

12. Complaints

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

13. Monitoring

The policy will be reviewed every two years 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

- Data protection policy
- Privacy notices for parents, pupils, staff, governors and suppliers
- Child Protection & Safeguarding policy
- Behaviour Policy

Appendix 1

Internal Access Protocols

1. **Incident occurs**

- An incident on the school grounds occurs in which CCTV should be reviewed.

2. **Request for footage**

- A Request for footage should be emailed to the System Manager.
- The Head Teacher and Deputy Head Teachers do not require permission to request footage.
- All other staff should get approval (via email) from the System Manager and Head Teacher for footage.

3. **Footage reviewed**

- System Manager to review footage on behalf of requester.
- System Manager to show footage to requester (if deemed appropriate).

4. **Footage released or stored**

- Footage can be released to Head Teacher or LT member (register of CCTV releases to be kept on behalf of the school by the System Manager).
- Footage can be released to other staff members if approved by the Head Teacher (release added to register).

5. **Footage deleted**

- Footage should be deleted when not required anymore. Once footage is deleted the CCTV release register should be updated on behalf of the school by the System Manager.