



CCTV and Surveillance Policy

Version number	2.0
Consultation groups	Central Executive Team, Head teachers, Data Protection Officer
Approved by	Board of Trustees
Approval date	
Adopted by	Advisory board
Adopted date	
Implementation date	September 2024
Policy/document owner	Data Protection Officer
Status	
Frequency of review	Annually
Next review date	July 2025
Applicable to	All Discovery Schools

Document History

Version	Version Date	Author	Summary of Changes
V1.0	September 2023	Zuber Ibrahim Assistant Head Teacher	<i>New policy prepared in line with:</i> <ul style="list-style-type: none"> ▪ <i>Data Protection Act 2018 and UK GDPR</i>
V2.0	September 2024	Zuber Ibrahim Assistant Head Teacher	<i>Removal of section referencing Bedroom Door Alarms</i>

1. Aims	2
2. Relevant legislation and guidance	3
3. Definitions.....	3
4. Covert surveillance.....	3
5. Location of the cameras.....	4
6. Roles and responsibilities.....	4
7. Operation of the CCTV system.....	5
8. Storage of CCTV footage	5
9. Access to CCTV footage.....	5
10. Data protection impact assessment (DPIA).....	7
11. Security.....	7
12. Complaints.....	7
13. Monitoring.....	7
Appendix 1: Millgate School CCTV request Flow chart.....	8

1. Aims

This policy aims to set out Millgate School’s approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property. CCTV footage is constituted as data, and as such is covered and protected under Data Protection law. Using data from CCTV should be seen as a last resort. In the first instance, witness testimony should hold sway. CCTV camera footage should only initially be used if no witnesses are present, or if an outside body (with the necessary permissions) such as the Police require the footage for an investigation or prosecution.

1.1 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
- 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 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 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.

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 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](#)

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

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 installed in and around the school building entrances, school playgrounds, carparks, perimeters and internal areas such as reception.

The planning and design of cameras endeavours 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 cameras are sited so that they only capture images relevant to the purposes for which they have been installed, 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.

Cameras are installed in such a way that they are not hidden from view. Warning signs will be clearly and prominently placed at the main external entrance to the school. In other areas where CCTV is used, the school will ensure that there are prominent signs placed within the controlled area.

6. Roles and responsibilities

6.1 The board of trustees

The board of trustees 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 Head teacher

The Head teacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the Local Data Protection Officer (LDPO) 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 LDPO 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 LDPO, whether to comply with disclosure of footage requests from third parties

6.3 The Local Data Protection Officer

The Local Data Protection Officer (LDPO) will:

- 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
- Receive and consider requests for third-party access to CCTV footage

6.4 The site manager

The site 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

6.5 The IT support and data team

The IT support and data team will:

- Support with request made to obtain data
- Oversee the storage of the CCTV footage
- Support with the IT system regarding CCTV for faults and security flaws

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 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.

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.

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.

9.1 Staff access

Authorisation to access CCTV footage must come from the Head teacher (with authorisation delegated to the Deputy Head teacher in the Head teacher's absence)

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

- The Local Data Protection Officer
- The IT support and data Team, whom receive request to obtain footage
- The site manager
- 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.

9.2 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.

Upon receiving the request the school will immediately issue a receipt and will then respond within 30 days.

All staff have received training to recognise SARs. When a SAR is received staff should inform the LDPO in writing. 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. We have the right to redact information, for example, on the basis of safeguarding.

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.

Footage will be uploaded to a secure folder; with details shared to authorised personnel.

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 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.

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 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 Trust DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by Adam Lapidge.

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 annually or whenever cameras are moved, 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 site manager will be responsible for overseeing the security of the surveillance system
 - 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

12. Complaints

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

13. 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.

Appendix 1: Millgate School CCTV request Flow chart

