GUISELEY SCHOOL

CCTV Policy

Approved on	Autumn Term 2023
Reviewed on	14 October 2025
Next review	Autumn Term 2026
Governors' committee	Resources
Responsible officer	Director of ICT and Data Services

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.

This policy outlines how Guiseley School uses CCTV in line with the principles set out within the Surveillance Camera Code of Practice 2021. All personal data obtained is stored in accordance with UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018.

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
- Monitor staff in the course of their normal duties, unless for specific disciplinary or investigatory reasons
- Follow or monitor 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.

Guiseley School will only 'covert record' when the following criteria are met:

- an assessment concluded that if we had to inform individuals that recording was taking place it would prejudice our objective
- there is reasonable cause to suspect specific criminal activity or actions that could result in a serious breach of staff or volunteer behavior expectations is taking place

5. Location of the cameras

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

Cameras are located in:

- General Teaching Building (All floors and externals)
- Sports and Arts Building (All floors and externals)
- F block (All floors and externals)
- Student Support Centre (All classrooms, corridor and externals)
- Bungalow (All classroom/meeting rooms and externals)
- Main Entrance Points (Pedestrian gate, vehicle gate and Back Lane gate)

Signage will be installed at the main entrance to each building and at entrance points to the site. 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

6.1 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.

6.2 The Headteacher

The headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system or delegate this to the system manager(s)
- Liaise with the data protection controller (DPC) 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 system manager(s) in the use of the system and from the DPC in data protection
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPC and taken into account the result of a data protection impact assessment
- Decide, in consultation with the DPC, whether to comply with disclosure of footage requests from third parties

6.3 The data protection controller

The data protection controller (DPC) will:

- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed when it falls out of the retention period
- 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 system is not infringing on any individual's reasonable right to privacy in public spaces
- Carry out annual 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

6.4 The system manager(s)

The system manager(s) 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
- 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

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 not record audio, with the exception of in the Isolation room. Recording access will be without audio by default. Access to audio recordings will be undertaken with authorisation from the Director of ICT and Data Services only.

Recordings will have date and time stamps. This will be checked by the system manager(s) 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 protected, so that the data will be secure and its integrity maintained, so that it can be used as evidence if required. All recordings must be logged and traceable throughout their life within the system.

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

8.1. CCTV System Security

A full Data Privacy Impact Assessment will be completed upon deployment, replacements, development or upgrading of the CCTV system. This is in line with the UK GDPR principle, Privacy by Design, and ensures the aim of the system is reasonable, necessary and proportionate.

The system will be made secure by the following safeguards:

- the system manager will be responsible for overseeing the security of the footage and recorded images, maintenance and training of authorised personnel
- the system will be check for faults each term
- the footage will be stored securely and encrypted
- the software updates will be installed as soon as possible
- the recorded footage will be password protected
- the equipment will be located in a secured lockable enclosure accessible only to authorised personnel
- adequate cyber security measures will be in place to protect footage from cyber-attacks
- a register of authorised staff is maintained, reviewed and updated when necessary

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.

With the exception of specific visual display monitors, footage will not be monitored ‘live’ as an ongoing process by system operators.

Any individuals that download footage or clips thereof must record their name, the date and time, and the reason for access in the access log by contacting the system manager/s.

Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

It will not be common practice to release CCTV footage unless satisfactory evidence for a secure legal basis can be provided. This is authorised within Section 115, Crime and Disorder Act 1998.

In appropriate circumstances, the school may allow authorised personnel to view footage where the above purposes are considered.

The school cannot guarantee disclosure of footage when made under a Subject Access Request due to:

- lack of technical resources available in order to blur or redact the footage
- the release of footage would prejudice an ongoing investigation
- other identifiable individuals have not consented

9.1 Staff access

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

- The Headteacher
- The senior leadership team
- The extended leadership team
- Pastoral teams
- Reception staff
- SENDCO/Deputy SENDCO
- The data protection controller
- The system managers (ICT Services and Site Team)

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 during term time. The school reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members.

All staff have received training to recognise SARs. When a SAR is received staff should inform the DPC 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.

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.

Information is sent a timed access link via OneDrive and this is password protected.

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 made in writing to the system manager, headteacher and be specific to a date and time frame.

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 DPC will consider very carefully how much footage to disclose, and seek legal advice if necessary.

The DPC will ensure that any disclosures will be done in line with UK GDPR and Data Protection. All disclosures will be recorded by the DPC.

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 DPC will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the director of ICT services.

A new DPIA will be done annually and/or 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. CCTV System Security

A full Data Privacy Impact Assessment will be completed upon deployment, replacements, development or upgrading of the CCTV system. This is in line with the UK GDPR principle, Privacy by Design, and ensures the aim of the system is reasonable, necessary and proportionate.

The system will be made secure by the following safeguards:

- The system manager/s will be responsible for overseeing the security of the CCTV system and footage and recorded images, maintenance and training of authorised personnel.
- 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.
- A register of authorised staff is maintained, reviewed and updated when necessary.

12. Complaints

Complaints should be made in accordance with the schools complaints policy.

13. Monitoring

The policy will be reviewed every three years by the Director of ICT and Data Services to consider whether the continued use of surveillance cameras remains necessary, proportionate and effective in meeting its stated purposes.