



BROWNEDGE ST MARY'S
CATHOLIC HIGH SCHOOL
'Let your light shine'

CCTV Policy

Signature of Head Teacher/

Date:

Chair of Governors:

Policy devised by: Mrs N Oddie

Date: February 2024

Review Date: February 2026

MISSION STATEMENT

Let your Light Shine

If we love others, we live in the light. 1 John 2:10

Inspired by our Gospel Values we have a shared responsibility to:-

- create an environment of welcome, love and respect for each member of our learning family.
- develop the unique gifts and talents of all, striving for excellence in everything we do.
- live out our commitment to love, service and justice in the local and global community.
- nurture the journey of faith and discovery for all.
- celebrate and reflect on the love of God, which is at the heart of all we are.

Rationale

Brownedge St Mary's Catholic High School believes that all pupils are entitled to learn in a safe and supportive environment. This policy outlines how we use CCTV to allow us to do this and our school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property. This policy applies to all personnel, and relates directly to the location and use of CCTV, the monitoring, recording and subsequent use of recorded materials.

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.

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)

Location of the cameras

Cameras are sited so they only capture images relevant to the purposes for which they are installed and care is 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 images captured comply with the GDPR regulations.

The system is owned by the school and comprises a number of fixed and moving cameras located around the school site. There are 60 cameras on the system 23 external and 37 internal.

The school makes every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

CCTV is not used in standard classrooms.

Members of staff have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

Covert Monitoring

The school may in exceptional circumstances set up covert monitoring. For example;

- where there is good cause to suspect that illegal or unauthorised action(s) are taking place, or where there are grounds to suspect serious misconduct.
- where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances authorisation must be obtained from the Headteacher. Covert monitoring must cease following completion of an investigation. Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example, toilets.

Roles and responsibilities

The Governing Body

The Governing Body has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation is complied with.

The Headteacher

The Headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the data protection officer (DPO) 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 DPO 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 DPO, whether to comply with disclosure of footage requests from third parties

The Data Protection Officer

The Data Protection Officer (DPO) 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 System Manager

The System 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

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.
- Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.
- Breaches of the policy by staff monitoring the system may constitute a disciplinary matter under the relevant conditions of employment.
- Any concerns in respect of the system's use or regarding compliance with this policy should be addressed to the Headteacher.

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.

If your process differs, detail how you will store footage here.

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

Control and access to the CCTV system

The Headteacher has overall responsibility for the control of images and deciding how the CCTV system is used.

The school's CCTV Scheme is registered with the Information Commissioner

Access to the CCTV system will be strictly limited to authorised operators with a password. It is accessible only by designated staff with responsibility for security, behaviour or attendance. Only people designated by the Headteacher may download / record CCTV images.

Unless in an immediate response to events, staff using the CCTV software must not direct cameras at an individual or a specific group.

Operators must satisfy themselves that all persons viewing CCTV material have the right to do so.

Access to the control of the CCTV system must be kept secure. Administrative functions will include controlling and maintaining downloaded digital materials, and maintenance and system access logs.

Any changes to CCTV monitoring will be subject to consultation with staff and the school community.

All operators and employees with access to images are aware of the procedures that need to be followed when accessing recorded images. This access includes viewing live images and remote playback but not the downloading / recording of data. All operators will receive training in respect of their responsibilities under the CCTV Code of Practice (<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-ofpractice.pdf>). All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

Any member of staff who misuses the surveillance system may be committing a criminal offence, and will face disciplinary action.

The following people have access to the cameras:

- Members of the Senior Leadership Team
- Network Manager
- Site Manager

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.

All requests for access should be set out in writing and sent to the headteacher and the DPO. Upon receiving a written 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 DPO 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. As a general rule, if the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed personal data. If it is not possible to conceal the identity of others, disclosure is unlikely.

The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

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

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 headteacher and the DPO.

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

The data may be used within the school's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.

All disclosures will be recorded by the DPO.

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 as stated at the beginning of this policy.

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 DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by person nominated by the Headteacher.

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 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.

Security

- The system 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
- 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

Complaints

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