

## Policy on use of CCTV

**Date:** reviewed Spring 2026; next review 2028

### Aims

This policy aims to set out Sphere Federation schools' approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property.

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
- 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 list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The school is registered with the Information Commissioner (ICO) as the data controller under the Data Protection Act 2018. The CCTV system operates under this registration.

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 the following legislation:

- [UK General Data Protection Regulation](#)
- [Data \(Use and Access\) Act 2025](#)
- [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](#)

This policy is based on the following guidance:

- [Surveillance Camera Code of Practice \(2021\)](#)

## Definitions

- Surveillance: the act of watching a person or a place
- CCTV: closed circuit television; video cameras used for surveillance
- Overt surveillance: surveillance which is clearly visible and signposted around the school and does not fall under the Regulation of Investigatory Powers Act 2000
- Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

## 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.

## Location of the cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (see above: Aims). Cameras are located in:

Scholes (Elmet) Primary	Moortown Primary	St James' CE Primary
<ul style="list-style-type: none"> <li>• car park</li> <li>• KS2 playground</li> <li>• adventure playground</li> <li>• Y5,6 building</li> <li>• walkway between swimming pool and KS2 corridor doors</li> <li>• KS1 top playground</li> <li>• out-of-school club / Nursery entrance area</li> <li>• Early Years play area</li> </ul>	<ul style="list-style-type: none"> <li>• front gate area</li> <li>• middle playground</li> <li>• middle playground</li> <li>• Y5,6 building main door and middle building cloakroom door</li> <li>• back playground / MUGA</li> <li>• back of Y5,6 building (triangle area)</li> <li>• front playground</li> </ul>	<p>(no cameras are installed)</p>

Appropriate signage is in place to warn members of the school community that they are under surveillance. 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.

## 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 (see above) is complied with.

### The Head of Federation and Head of School

The Head of Federation and Head of School:

- 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
- ensures staff recognise a subject access request
- deals with subject access requests in line with the Data Protection Act 2018 and the Freedom of Information Act (2000)

- 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 Sphere Federation Resources Manager and/or Data Protection Officer**

The Sphere Federation Resources Manager acts as the Data Protection Lead for Sphere Federation schools. With appropriate support from the Data Protection Officer and the Head of Federation, the Sphere Federation Resources Manager:

- monitors compliance with UK data protection law
- conducts or assists the school with carrying out data protection impact assessments
- acts as a point of contact for communications from the Information Commissioner's Office
- conducts data protection impact assessments
- ensures data is handled in accordance with data protection legislation
- ensures footage is obtained in a legal, fair and transparent manner
- ensures footage is destroyed when it falls out of the retention period
- keeps accurate records of all data processing activities and make the records public on request
- informs 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
- ensures 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
- ensures that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- carries out checks to determine whether footage is being stored accurately, and being deleted after the retention period
- receives and considers requests for third-party access to CCTV footage

## **The system manager**

The system manager:

- take care of the day-to-day maintenance and operation of the CCTV system
- oversees the security of the CCTV system and footage
- checks the system for faults and security flaws
- ensures the data and time stamps are accurate

## **Operation of the CCTV system**

- The CCTV system is operational 24 hours a day, 365 days a year.
- The system does not record audio.
- Recordings have date and time stamps; this is checked by the system manager and when the clocks change.

## **Storage of CCTV footage**

In accordance with the Data (Use and Access) Act 2025, data must be deleted once it is no longer necessary for its original purpose. Footage is retained for 21 days (Scholes (Elmet) Primary) or 30 days (Moortown Primary). At the end of the retention period, the files are overwritten automatically.

On occasion footage may be retained for longer eg 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 are downloaded and encrypted so that the data is secure and its integrity maintained, so that it can be used as evidence if required.

## **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 are positioned so only authorised personnel will be able to see the footage.

## **Staff access**

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

- Head of Federation
- Head of School

- Deputy Head of School
- Data Protection Officer (Bywater Kent Ltd)
- The system manager
- Anyone with express permission of the Head of Federation

CCTV footage is only accessed 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.

### **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 will then respond within 30 school days. The school reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members.

Staff have received training to recognise SARs. When a SAR is received, staff 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 eg if 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 eg by blurring out 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, 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.

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 (see above: Aims).

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 (eg investigators).

All requests for access should be set out in writing and sent to the Head of Federation 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 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 (see above: Aims).

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 the Data Protection Lead in school.

Those whose privacy is most likely to be affected 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.

## Security

- The system manager is responsible for overseeing the security of the CCTV system and footage.
- Scholes (Elmet) Primary: The system is checked for faults frequently; Moortown Primary: The system is checked on an ongoing basis.
- Any faults in the system are 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 are put in place to protect the footage from cyber-attacks.
- Software updates are automatically rolled out as and when required, and are checked annually during maintenance visits.

## Complaints

If you wish to raise a complaint about how we manage your personal data, please refer to our Data Protection Policy for further information on the complaints process.

## Monitoring

The policy is 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.

## Links to other policies

This policy links with various other Sphere Federation policies, which include:

- Freedom of Information Policy
- Data Protection Policy
- Privacy notices for parents, pupils, staff, governors, volunteers and applicants
- Safeguarding and Child Protection Policy

This list is not exhaustive.