

Policy Name	CCTV
Policy Type	Discretionary
Issue Date	3 rd December 2024
To Be Reviewed	Bi-annually: 3 rd December 2026
Approved by	CEO
Policy Owner	Chris Roberts

Glossary of Abbreviations and Acronyms used in this Policy

Closed Circuit Television (CCTV)	Information Controlling Officer (ICO)
Data Protection Officer (DPO)	Information Technology (IT)
General Data Protection Regulation (GDPR)	Subject Access Request (SAR)

Policy Statement

Orbis Education Trust uses Closed Circuit Television (CCTV) within its premises. The purpose of this policy is to set out the position of the trust as to the management, operation and use of the CCTV.

This policy applies to all members of our workforce, visitors to the trust premises and all other persons whose images may be captured by the CCTV system.

This policy takes account of all applicable legislation and guidance, including:

- General Data Protection Regulation (GDPR).
- Data Protection Act 2018 (together the Data Protection Legislation).
- CCTV Code of Practice produced by the Information Commissioner.
- Human Rights Act 1998.

This policy sets out the position of the trust in relation to its use of CCTV.

Purpose of CCTV

The trust uses CCTV for the following purposes:

- To provide a safe and secure environment for students, staff and visitors.
- To prevent the loss of or damage to the trust buildings and/or assets.
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders.
- To monitor the security of the site.

Description of System

The system consists of fixed dome and bullet cameras that record video only.

Siting of Cameras

All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, students and visitors.

Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The trust will make all reasonable efforts to ensure that areas outside of the trust premises are not recorded.

Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets. Cameras will be used, in both schools, in some classrooms in order to mitigate damage (e.g. IT suites), for safety reasons (e.g. food technology rooms), in corridors and outside locations.

Privacy Impact Assessment

Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the trust to ensure that the proposed installation is compliant with legislation and ICO guidance.

The trust will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

Management and Access

CCTV systems will be managed by the IT Services Director and the Headteachers of both schools.

On a day to day basis the CCTV system, within Orbis Education Trust, is managed by operated by the IT Services Team. At both Southfield School and Kingsthorpe College the system is operated by the Headteacher and Deputy Headteacher with responsibility for behaviour and safeguarding.

The viewing of live and recorded CCTV images, within Orbis Education Trust, will be restricted to only those members of staff with responsibility for behaviour and/or safeguarding at the direction of the Executive Director (IT), Headteacher and Deputy Headteacher with responsibility for behaviour and safeguarding at both schools.

No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

The CCTV systems, within Orbis Education Trust, are checked weekly by the Executive Director (IT) to ensure that they are operating effectively.

Storage and Retention of Images

Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

Recorded images are stored for a period of no longer than 30 days unless there is a specific purpose for which they are retained for a longer period.

The trust will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

- CCTV recording systems being located in restricted access areas.
- The CCTV system being encrypted/password protected.
- Restriction of the ability to make copies to specified members of staff.
- A log of downloaded CCTV images will be maintained by the trust and kept in a secure manner.

Disclosure of Images to Data Subjects

Any individual recorded in any CCTV image is a data subject, for the purposes of the Data Protection Legislation, and has a right to request access to those images.

Any individual who requests access to images of themselves will be considered to have made a Subject Access Request (SAR) pursuant to the Data Protection Legislation. Such a request should be considered in the context of the trust's Subject Access Request (SAR) Policy.

When such a request is made, the Executive Director (IT), the Headteacher and Deputy Headteacher with responsibility for behaviour and safeguarding at both schools will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The Executive Director (IT), the Headteacher and Deputy Headteacher with responsibility for behaviour and safeguarding at both schools must take appropriate measures to ensure that the footage is restricted in this way.

If the footage contains images of other individuals, then the trust must consider whether:

- The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals.
- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or
- If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

A record must be kept, and held securely, of all disclosures which sets out:

- When the request was made.
- The process followed by the relevant staff in determining whether the images contained third parties.
- The considerations as to whether to allow access to those images.
- The individuals that were permitted to view the images and when; and
- Whether a copy of the images was provided, and if so to whom, when and in what format.

Disclosure of Images to Third Parties

The trust will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

If a request is received from a law enforcement agency for disclosure of CCTV images then the relevant staff must follow the same process as above in relation to Subject Access Requests. Details should be obtained from the law enforcement agency as to exactly what they want the CCTV images for and any particular individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

The information above must be recorded in relation to any disclosure.

If an order is granted by a court for disclosure of CCTV images, then this should be complied with. However, very careful consideration must be given to exactly what the court order requires. If there are any concerns as to disclosure, then the Data Protection Officer (DPO) should be contacted in the first instance and appropriate legal advice may be required.

Review of Policy and CCTV System

The CCTV system and the privacy impact assessment relating to it will be reviewed BIENNUELY.

Misuse of CCTV systems

The misuse of CCTV system could constitute a criminal offence.

Any member of staff who breaches this policy may be subject to disciplinary action.

Complaints relating to this policy

Any complaints relating to this policy or to the CCTV system operated by the trust should be made in accordance with the Trust Complaints Policy.

ENCLOSURE 1: CCTV PRIVACY IMPACT ASSESSMENT

1. Who will be captured on CCTV?

Students, staff, parents/carers, volunteers, trustees, governors and other visitors; including members of the public, etc.

2. What personal data will be processed?

Facial Images, behaviour.

3. What are the purposes for operating the CCTV system? Set out the problem that the trust is seeking to address and why the CCTV is the best solution and the matter cannot be addressed by way of less intrusive means.

Prevention or detection of crime, the apprehension and prosecution of offenders, safeguarding students, staff and public safety, to assist in managing student behaviour and to monitor the security of the site.

4. What is the lawful basis for operating the CCTV system?

Legal obligation, legitimate interests of the organisation to maintain health and safety and to prevent and investigate crime.

5. Who is/are the named person(s) responsible for the operation of the system?

The Chief Executive Officer.
The Headteachers.
The Deputy Headteachers with responsibility for Safeguarding
The Executive Director (IT).

6. Describe the CCTV system, including:

Cameras are located on public corridors or in rooms where there are potential security or health and safety issues.

7. Set out the details of any sharing with third parties, including processors.

The trust will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation. CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

8. Set out the retention period of any recordings, including why those periods have been chosen.

30 days

9. Set out the security measures in place to ensure that recordings are captured and stored securely.

See policy

10. What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

See policy

11. What measures are in place to address the risks identified?

See policy

12. Have parents and students, where appropriate, been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

Notices have been placed around the sites.

13. When will this privacy impact assessment be reviewed?

Biennially.