CCTV POLICY

Bishop Martin CE Primary

OUR TRUST'S PRAYER

Heavenly Father,

Let peace, friendship and love grow in our schools.

Send the Holy Spirit to give

excellence to our learning,

love to our actions and

joy to our worship.

Guide us to help others,

so that we may all

Learn, Love and Achieve, Together with Jesus.

Amen

1 Policy Statement

1.1 The Liverpool Diocesan Schools Trust ("the Trust") uses Closed Circuit Television ("CCTV") within the premises of Bishop Martin CE Primary School {"the school"). The purpose of this policy is to set out the position of the Trust as to the management, operation and use of the CCTV at the school.

1.2 This policy applies to all members of our Workforce, visitors to the school's premises and all other persons whose images may be captured by the CCTV system.

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

1.3.1 General Data Protection Regulation ("GDPR")

1.3.2 Data Protection Act 2018 (the Data Protection Legislation)

1.3.3 CCTV Code of Practice produced by the Information Commissioner

1.3.4 Human Rights Act 1998

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

2 Purpose of CCTV

2.1 The school uses CCTV for the following purposes:

2.1.1 to prevent crime, protect buildings and assets from damage, disruption, vandalism and other crime;

2.1.2 for the personal safety of pupils, staff, visitors and other members of the public and to act as a deterrent against crime;

2.1.3 to support law enforcement bodies in the prevention, detection and prosecution of crime;

2.1.4 to assist in the day-to-day management of the school including ensuring the health and safety of pupils, staff and others;

2.1.5 for pupil/student behaviour management (discipline and exclusions); and

2.1.6 to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings and associated processes and appeals

3 Description of system

3.1 We have fifteen fixed cameras that only record pictures for internal use (they are not equipped for sound recording). They are located strategically within the boundaries of the school grounds and two internal cameras; the two internal cameras are located at the school reception and the main corridor into school. There are 13 external cameras.

4 Siting of Cameras

4.1 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, pupils and visitors.

4.2 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 school will make all reasonable efforts to ensure that areas outside of the school's premises are not recorded.

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

4.4 Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets.

5 Privacy Impact Assessment

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

5.2 The school 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.

6 Management and Access

6.1 The CCTV system will be managed by the Executive Headteacher.

6.2 On a day to day basis the CCTV system will be operated by Techminder.

6.3 The viewing of live CCTV images will be restricted to the Senior Leadership Team.

6.4 Recorded images which are stored by the CCTV system will be restricted to access by the Senior Leadership Team.

6.5 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.

6.6 The CCTV system is checked Daily by the Site Manager to ensure that it is operating effectively. It is also serviced on annual basis by Unique Integrated Systems.

7 Storage and Retention of Images

7.1 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.

7.2 Recorded images are stored only for a period of 15 days unless there is a specific purpose for which they are retained for a longer period.

7.3 The school 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:

7.3.1 CCTV recording systems being located in restricted access areas;

7.3.2 The CCTV system being encrypted/password protected;

7.3.3 Restriction of the ability to make copies to specified members of staff

7.4 A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the school.

8 Disclosure of Images to Data Subjects

8.1 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.

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

8.3 When such a request is made the Senior Leadership Team will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

8.4 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 Senior Leadership Team must take appropriate measures to ensure that the footage is restricted in this way.

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

8.5.1 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;

8.5.2 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

8.5.3 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

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

8.6.1 When the request was made;

8.6.2 The process followed by the Senior Leadership Team in determining whether the images contained third parties;

8.6.3 The considerations as to whether to allow access to those images;

8.6.4 The individuals that were permitted to view the images and when; and

8.6.5 Whether a copy of the images was provided, and if so to whom, when and in what format.

9 Disclosure of Images to Third Parties

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

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

9.3 If a request is received form a law enforcement agency for disclosure of CCTV images then the Senior Leadership Team must follow the same process as above in relation to subject access requests. Detail 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.

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

9.5 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 should be contacted in the first instance and appropriate legal advice may be required.

10 Misuse of CCTV systems

10.1 The misuse of CCTV system could constitute a criminal offence.

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

11 Complaints relating to this policy

11.1 Any complaints relating to this policy or to the CCTV system operated by the school should be made in accordance with the school's Complaints Policy.

Review Schedule

Policy Author	Data Protection Officer (DPO)
Policy Approver	Audit and Risk Committee
Current Policy Version	1.5
Policy Effective From	June 2026
Policy Review Date	June 2027

Revision Schedule

Version	**Revisions**	**By whom**
1.0	Original document produced	DPO
1.1	Minor updates to contact information	DPO
1.2	None	DPO
1.3	Minor changes to branding.	DPO
1.4	Added CCTV DPIA as an appendix – internal use.	DPO
1.5	Updated purposes within clause 2.1 and Step 1 of the DPIA.	DPO