CCTV Policy

Committee Lead:	**Finance and Business Operations**
Adopted:	December 2020
Date of next review:	December 2022

Signed by Chair of Trustees:

CCTV POLICY

1 Policy Statement

1.1 Within MITRE, some schools use Close Circuit Television ("CCTV") within the premises of the school. The purpose of this policy is to set out the position of the school 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 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]* (together 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 National School 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 provide a safe and secure environment for students, staff and visitors

2.1.2 To prevent the loss of or damage to the school buildings and/or assets

2.1.3 To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

3 Description of system

3.1 There are 30 cameras. All of the cameras are fixed, they do not rotate. There is sound recording on one internal camera situated in main reception but the sound is turned off, all other cameras only have live image recording. It is possible to obtain a still image and video clips from the live recordings.

3.2 Currently static internal CCTV cameras situated ICT corridor, Computer rooms 1, 2, 3, 4 and 5, room 29, main reception and Inclusion department.

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, students 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 premises are not recorded.

4.3 Signs will be in place which 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 IT support.

6.2 On a day to day basis the CCTV system will be operated by site manager, DPO or IT support.

6.3 The viewing of live CCTV images will be restricted to the Senior Leadership Team; Data Protection Officer (DPO) and the site manager. CCTV may only be viewed by staff for the purposes described in section 2.

6.4 Recorded images which are stored by the CCTV system will be restricted to access by the Senior Leadership Team; DPO and site manager or as required under reasonable discretion of the Principal or DPO in conjunction with the CEO.

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.

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 7 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 relevant DPO will oversee the request to review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request, allocating the task as required to others who are listed in 6.3.

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 DPO 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 DPO 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 or in accordance with paragraph 6.4.

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 from a law enforcement agency for disclosure of CCTV images then an individual as named in 6.3 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.

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 Review of Policy and CCTV System

10.1 This policy will be reviewed biennially.

10.2 The CCTV system and the privacy impact assessment relating to it will be reviewed biennially. See Annex A for privacy impact statement of The National Church of England School.

11 Misuse of CCTV systems

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

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

12 Complaints relating to this policy

12.1 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.

Annex A

CCTV PRIVACY IMPACT ASSESSMENT December 2020 – December 2022

1 Who will be captured on CCTV?

Students, staff, parents / carers, volunteers, Governors and other visitors including members of the public

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 School 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 and to maintain a safe environment

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

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?

DPO, Leadership team and site manager (supported by ICT technicians)

6 Describe the CCTV system, including:

a. how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained;

1. CCTV installed a number of years ago and was chosen because of the quality of images it produces.

b siting of the cameras and why such locations were chosen;

2. to cover the main areas of the school, particularly focussed on areas where preventing crime and health and safety may be a focus, such as around toilet areas, main corridors and entrances to the school

c how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;

3. cameras are focussed on school grounds, some images are captured of public near the front entrance

d where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and

4. there are notices on each entrance into the school, chosen to inform anyone entering the building that their image is captured

e whether the system enables third party data to be redacted, for example via blurring of details of third party individuals.

5. The system does not currently allow for redacting

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

Police, subject access requests.

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

One week, as per GDPR guidance

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

Accessed on computers which are password protected

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

Risks: • Is it fair to record them in the way proposed? We consider that it is fair to record individuals who are fully informed that this is the case. Cameras are not placed in toilets or changing rooms or any classrooms or halls, they are in public spaces only. • How is the amount of data processed to be minimised? The recordings are only kept for one week (reduced from one month to support the GDPR requirements). • What are the risks of the system being accessed unlawfully? Unlawful access may give information that certain individuals were on site, but this isn't always easy to see as students often move in crowds. Cameras would not give inappropriate images as they are only located in public areas. • What are the potential data breach risks? A breach would rely upon an unauthorised person accessing the system – this is password controlled. A breach may rely upon an unauthorised person entering the building (which is secure) then accessing the system which has a password control. However, if a breach did occur the risk is minimal, other than being able to establish that an individual was on site at any particular time and date over the period for which the data is retained (one week) • What are the risks during any transfer of recordings, or when disclosed to third parties such as the police? That data is not redacted and therefore discloses more than required. However the risk associated is minimal, it would only disclose that any individual had been on site at a date and time.

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

Site access is limited to authorised people. CCTV system is limited access. Log is retained of access to the images. Images are overwritten on a 7 day cycle. Images only capture people in public areas.

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?

Unable to comment whether this was performed before installation. However it has not been done recently as it seems not to be applicable for a system that is already in place. The privacy statements declare that we capture images of those on site.

13 When will this privacy impact assessment be reviewed?

December 2022

Approval:

This assessment was approved by the Data Protection Officer:

DPO ……

Date …….