ISLEWORTH & SYON SCHOOL
FINIS CORONAT OPUS

KEY POLICY

# CCTV

| | | | |
|---|---|---|---|
| **DRAFTED BY:** | T Billimoria | **STATUS:** | Guidance |
| **APPROVED:** | Trustees | **GOV. PANEL:** | Full Trustees |
| **ISSUE:** | 2 | **NEXT REVIEW:** | As required |

## Contents



## 1. Policy Statement

**1.1.** Isleworth & Syon School uses Closed-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 students, 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:

- General Data Protection Regulation ("GDPR")
- Data Protection Act 2018 (together with other Data Protection Legislation)
- Surveillance Camera Code of Practice 2021
- Human Rights Act 1998

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

## 2. Definitions

| | |
|---|---|
| Surveillance: | the act of watching a person or a place |
| CCTV: | closed circuit television; fixed video cameras used for surveillance |
| Personal data: | data relating to a living individual who can be identified from that data; for the purposes of this policy, video images of identifiable individuals |
| Data users: | authorised members of staff whose work involves processing personal data. This includes those whose duties are to operate CCTV cameras to record, monitor, store, retrieve and delete image. Data users must protect the data they handle in accordance with this policy and our Data Protection Policy |
| Data controllers: | a person or organisation who determines the purposes and means of the processing of personal data. The data controller for the CCTV is identified as Isleworth & Syon School |
| Processing: | any activity which involves the use of data; this includes obtaining, recording or holding data or carrying out any operation on the data, including amending, retrieving, using, disclosing or destroying it. This includes transferring personal data to third parties. |

## 3. Purpose of CCTV

**3.1.** The School uses CCTV for the following purposes:

**3.1.1.** To provide a safe and secure environment for students, staff and visitors

**3.1.2.** To prevent the loss of, or damage to, the School buildings and/or assets

**3.1.3.** To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

**3.1.4.** To assist, where relevant, in litigation proceedings

**3.1.5.** To assist in the effective resolution of disputes which may arise in the course of staff disciplinary and grievance proceedings

**3.2.** The CCTV system will not be used to:

**3.2.1.** Encroach on an individual's right to privacy

**3.2.2.** Follow particular individuals or groups on the live feed, unless there is an ongoing emergency incident occurring or to monitor risk to safety of individuals or property while carrying out a process

**3.2.3.** Pursue any other purposes than the ones stated above.

## 4. Description of System

**4.1.** The latest system, installed over 2017-20 is computer-based. The external cameras have an infra-red capacity to enhance night-time security. The system does not record sound.

**4.2.** A range of fixed internal and external cameras (both dome-style and bullet-style) give very good coverage of the whole school estate 24 hours a day.

## 5. Location of Cameras

**5.1.** 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.

**5.2.** 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. Cameras are not and will not be aimed off school grounds into private properties

**5.3.** Signs are in place to inform individuals that they are in an area within which CCTV is in operation. Reception sign identifies the school as the operator and data controller and provides a point of contact.

**5.4.** In areas where individuals have a heightened expectation of privacy, such as changing rooms or enclosed toilet cubicles, entrances/exits to such facilities may be covered by CCTV but an individual's right to privacy will be ensured.

## 6. Data Privacy Impact Assessment (DPIA)

**6.1.** When the CCTV system is replaced, developed or upgraded, a Data Privacy Impact Assessment will be conducted by the School to ensure that the proposed installation is justifiable, necessary, proportionate, and compliant with legislation and Information Commissioner's Office (ICO) guidance.

## 7. Roles and Responsibilities

**7.1.** The Trustees have ultimate responsibility for oversight of the CCTV system, and how it is operated in accordance with this policy, ensuring relevant legislation is complied with

**7.2.** The Co-Headteachers have responsibility for all day-to-day leadership and management of the CCTV system

**7.3.** The CCTV system will be managed by a member of the School's Senior Leadership Team.

**7.4.** On a day-to-day basis the CCTV system will be maintained and operated by the School's Network Manager

**7.5.** Where necessary, the data protection officer (DPO) will advise on and assist the school with carrying out Data Protect Impact Assessments (DPIA) and Subject Access Requests

## 8. Access

**8.1.** The viewing of live CCTV images will be restricted to members of the School's Senior Leadership Team; members of the School's Pastoral Team; the School's Premises Team, the Network Team and the School Librarian. Access for the School Librarian is restricted to the library only. These are the identified data users.

**8.2.** Recorded images stored by the CCTV system will also be restricted to access by those listed in 8.1.

**8.3.** No other individual will have the right to view or access any CCTV images unless in accordance with the purposes of the policy listed in 3.1, and the terms of this policy as to disclosure of images.

## 9. Security

**9.1.** The Network Manager will be responsibility for overseeing the security of the CCTV system

**9.2.** The system will be checked termly and when clocks change for:

- Faults and security flaws
- ensuring that date/time stamps are accurate

**9.3.** Any faults in the system will be reported to the Network Team/Site Team as soon as they are detected

**9.4.** 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;

- CCTV recording systems being located in restricted access areas: specifically, the main server room which is physically secure. Access is limited to the Network Team, Premises Team, Co-Headteachers and member of the School's Senior Leadership Team overseeing management of the CCTV system
- The CCTV system being password protected
- Downloaded recordings are exported to mp4 files or saved as videos within PowerPoint. These both follow the same encryption standard as all other files on staff laptops and desktops (BitLocker full disk encryption)
- Restriction of the ability to make copies to specified members of staff as listed in section 8.1
- The two NVR CCTV systems are their own dedicated servers to protect footage from cyber attacks
- CCTV cameras are on their own physical network to ensure they are separate from the rest of our network
- Security updates published by Hikvision will be applied as soon as possible
- Staff training provided to users listed in 8.1 on the purpose and correct use of the CCTV system to ensure adherence to this policy. Rules for use will be explicitly shared in this training.

## 10. Storage and Retention of Images

**10.1.** Any images recorded by the CCTV system will be retained only for a period of 8 weeks. This time frame is used so that it covers all school holiday periods. If, under 12.6 a request for footage has been made and agreed to for court proceedings, it will not be destroyed.

## 11. Disclosure of Images to Data Subjects

**11.1.** 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.

**11.2.** 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 a Subject Access Request under the School's Data Protection Policy

**11.3.** When such a request is made members of staff listed in 8.1 will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

**11.4.** 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 members of staff listed in section 8.1 must take appropriate measures to ensure that the footage is restricted in this way.

**11.5.** If the footage contains images of other individuals, then the School 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.

**11.6.** 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.

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

- When the request was made;
- The process followed by the member of staff accessing the footage (limited to those listed in section 8.1) 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. Footage disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

## 12. Disclosure of Images to Third Parties

**12.1.** The School will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with Data Protection Legislation,

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

**12.3.** All requests should be set out in writing and sent to the Co-Headteachers. The Co-Headteachers will contact the Data Protection Officer to establish if a Data Sharing Agreement should be completed

**12.4.** If a request is received from a law enforcement agency for disclosure of CCTV images, then the member of staff (limited to those listed in section 8.1) 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.

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

**12.6.** If an order is granted by a Court for disclosure of CCTV images, then this should be complied with without giving unrestricted access. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to the disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

## 13. Misuse of CCTV systems

**13.1.** The misuse of CCTV system could constitute a criminal offence.

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

## 14. Complaints Relating to this Policy

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.

## 15. Other Relevant School Policies

The following policies and procedures are also relevant to this Policy.

- Data Protection Policy
- Complaints Policy

## 16. Legislation

The following legislation is relevant to this Policy.

- Data Protection Act 2018
- Surveillance Camera Code of Practice 2021
- Human Rights Act 1998

## 17. Retention and Data Protection

Through the application of this policy, the School may collect, process and store personal data in accordance with our data protection policy. We will comply with the requirements of the Data Protection Legislation (being (i) unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998). Records will be kept in accordance with our Privacy Notices, our Retention & Destruction Policy and in line with the requirements of the Data Protection Legislation.

## 18. Reviewing

**18.1.** Trustees and the Senior Leadership Team will review this policy as required, to ensure the effectiveness and compliance of the procedure, and make changes where necessary

**18.2.** The CCTV system will be audited annually to ensure the system remains necessary, proportionate and effective in meeting its stated purpose.

## Appendix 1 – CCTV Data Privacy Impact Assessment

1. **Who will be captured on CCTV?**
   Students, staff, parents/carers, volunteers, Governors, contractors and other visitors, including members of the public.

2. **What personal data will be processed?**
   Facial images and full and/or part body 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.**

   - To enhance safety for all students and staff and other visitors, on the school site. The system is to provide some security for members of the school community through the knowledge that the school estate has good CCTV coverage. The system also allows for any incidents to be properly investigated with some surety that observations can clarify certain incidents.

   - The prevention or detection of crime. The system will support the aim by acting as a deterrent and also providing supporting evidence should a crime take place.

   - To assist crime prevention agencies in investigating crimes. Recorded images will support agencies in investigating and solving crimes.

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?**
   Names individuals can be found on the Key Personnel list. The current positions for operation of the system are:

   - Assistant Headteacher – manages the system
   - Senior Network Manager – operates the system

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;**
   b. **siting of the cameras and why such locations were chosen;**
   c. **how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;**
   d. **where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and**
   e. **whether the system enables third party data to be redacted, for example via blurring of details of third-party individuals.**

   a. The system was chosen following a tendering process that included analysis of the images produced. The cameras were trialled prior to installation to ensure that the quality was suitable for proper identification of individuals.

   b. The cameras have been carefully sited to ensure a full coverage of the school's site, including the grounds, around the buildings, internal corridors and stairwells and classrooms in support of our stated purpose of the CCTV system

   c. Cameras have been carefully sited so as to cover the school grounds and buildings, including areas of potential vulnerability. In certain instances, sections of the video are covered with black boxes in order to retain privacy.

   d. Signage is currently in place at the entrances to the school grounds.

   e. The system allows for images to be redacted.

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

   - Images might be shared, by request, with the Police.
   - We do not intend to use any other provider in relation to the CCTV system but will manage the system in school.

8. **Set out the retention period of any recordings, including why those periods have been chosen**
   The retention period will be up to 8 weeks. This is so that school holiday periods are fully covered. Holiday periods do leave the school estate more susceptible to crime and this period of time should allow sufficient coverage for crimes to be noticed and investigated.

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

- The main server room is physically secure and access is limited to the Network Team, Site Team, Co-Headteachers and member of the School's Senior Leadership Team overseeing management of the CCTV system.
- Access to live and recorded images is password protected.
- Downloaded recordings are exported to mp4 files and have BitLocker full disk encryption (standard across all school desktops and laptops)
- The two NVR CCTV systems are their own dedicated servers to protect footage from cyber attacks
- CCTV cameras are on their own physical network to ensure they are separate from the rest of our network
- Security updates published by Hikvision will be applied as soon as possible
- If hard-drives need to be disposed of then this is done in a secure manner and in line with the school's ICT policy.
- Staff training is in place which will train those staff mentioned in section .7.1 on the purpose and correct use of the CCTV system to ensure adherence to this policy

10. **What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?**
We consider it fair to record those on the school site as student/staff/visitor safety is of paramount importance to the school. The recording of images is for the protection of all members of the school community.

The amount of data is minimised in how the data is stored and disposed of. There is no desire to retain redundant information beyond the 8-week period set out in this policy.

Security measures are in place to ensure that the system cannot be accessed unlawfully. It is clear in this policy how protections have been considered and put in place.

The potential data breach risks are if restricted people are given access to the recorded images. It is considered that this risk is minimal.

The potential risks during transfer to third parties are that excessive data is passed on. A member of the school's staff team will be responsible for ensuring that this is not the case and that only relevant images are forwarded in this way.

11. **What measures are in place to address the risks identified?**
The system is managed by a senior member of staff with responsibility for ensuring that the system is secure and safe.

Colleagues with access to the system are only those who may have cause to search images as part of their job responsibilities.

The whole system is properly protected with physical security and through network permissions and passwords.

12. **Have parents and pupils 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?**
When the original system was installed, consultation took place through the Parent Teachers' Association, prior to the installation of the system.

Information was given about the installation of the new system to parents/carers.

13. **When will this privacy impact assessment be reviewed?**
This privacy impact assessment will be reviewed every two years.

## APPROVAL

This assessment was approved by the Data Protection Officer:

| | | | |
|---|---|---|---|
| **SIGNATURE:** | | **DATE:** | |