



# **CCTV Policy**

## **September 2023**

## Contents

1	Policy statement
2	Purpose of CCTV
3	Description of System
4	Siting of Cameras
5	Privacy Impact Assessment
6	Management & Access
7	Storage and Retention of Images
8	Disclosure of Images to Data Subjects
9	Disclosure of Images to Third Parties
10	Review of Policy and CCTV System
11	Misuse of CCTV systems
12	Complaints relating to this policy

## Annex

### Trust Mission Statement

We are a partnership of Catholic schools, and our aim is to provide the very best Catholic education for all in our community and so improve life chances through spiritual, academic, and social

development. We will achieve this by:

- Placing the life and teachings of Jesus Christ at the centre of all that we do
- Following the example of Our Lady of Lourdes by nurturing everyone so that we can all make the most of our God given talents
- Working together so that we can all achieve our full potential, deepen our faith, and know that God loves us
  - Being an example of healing, compassion, and support for the most vulnerable in our society

*Psalm 138: 7 (GNT)*

*When I am surrounded by troubles, you keep me safe.  
You oppose my angry enemies and save me by your power.*

## **Guidance Note for School Leaders/Site Managers:**

A key element in the assessment of lawful use of CCTV systems is the privacy impact assessment (PIA) conducted in relation to those systems setting out the justification for the system and its compliance with data protection legislation.

If the Trust/School has not conducted such an assessment then this must be conducted now, and this template policy amended to take account of the outcome of that assessment.

The Trust/School should do this with an open mind, including considering whether any existing cameras should be removed, or the system modified in any way.

The completed impact assessment template should be forwarded to the Trust DPO for sign-off/approval.

- Highlighted sections of the policy should be completed as appropriate for each setting
- The Headteacher should designate named staff members to access / view the CCTV images
- The designated manager of the CCTV system should retain the log of access to viewed images (this log should be available as part of the GDPR annual audit)
- The designated manager of the CCTV system should retain the log of disclosures to third parties (this log should be available as part of the GDPR annual audit)

## **1 Policy Statement**

1.1 St Peter St Paul Catholic Voluntary Academy (SSPP) uses Close Circuit Television (“CCTV”) within the premises of SSPP. The purpose of this policy is to set out the position of SSPP as to the management, operation and use of the CCTV at SSPP.

1.2 This policy applies to all members of our Workforce, visitors to SSPP 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 SSPP in relation to its use of CCTV.

## **2 Purpose of CCTV**

2.1 SSPP uses CCTV for the following purposes:

2.1.1 To provide a safe and secure environment for pupils, staff, and visitors

2.1.2 To prevent the loss of or damage to SSPP buildings and/or assets and assist with any related financial claims/recovery

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

2.1.4 To assist in the enforcement of the behaviour policy at SSPP through verifying witness statements and observing the severity of an incident.

## **3 Description of system**

3.1 There are 52 fixed non-PTZ cameras situated around the site of SSPP.

3.2 Cameras are situated to cover both indoor and outdoor areas.

3.3 All cameras have a name to identify them. This, along with the current date and time, is watermarked onto all CCTV footage.

3.4 It is the aim of SSPP to cover all indoor and outdoor spaces for the purposes described in 2.1. This excludes areas with increased expectation of privacy (Such as changing rooms, toilet urinals and toilet cubicles) and classrooms.

3.5 The cameras installed indoors have sound recording capability.

## **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. SSPP will make all reasonable efforts to ensure that areas outside of SSPP premises are not recorded. In cases where this is not possible, SSPP will use the CCTV software to block off a part of the video feed so as not to record the third-party premises.
- 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 SSPP to ensure that the proposed installation is compliant with legislation and ICO guidance.
- 5.2 SSPP will adopt a privacy by design approach when installing new cameras and systems, considering the purpose of each camera to avoid recording and storing excessive amounts of personal data.

## **6 Management and Access**

- 6.1 The CCTV system will be managed by Mr P Archer.
- 6.2 On a day-to-day basis the CCTV system will be operated by Mr P Archer.
- 6.3 The viewing of live CCTV images will be restricted to the Senior Management Team, Site Team, IT Team, Pastoral Staff and Reception Staff.
- 6.4 Access to recorded images which are stored by the CCTV system will be restricted to the Senior Management Team, Site Team, IT Team, and Pastoral Staff.
- 6.5 Additionally, IT support staff may also view live or recorded CCTV images to aid authorised staff in accordance with this policy e.g., finding footage of an event in the recorded images or downloading recorded images for viewing by authorised staff.
- 6.6 Where deemed appropriate by staff in 6.3 and 6.4, live CCTV images and recorded CCTV images may be shared with other members of SSPP staff body for the purposes of:
  - 6.6.1 Identifying an individual where the accessing staff member is unable to identify them.
  - 6.6.2 Observing the severity of an incident for the purposes of administering first aid.
  - 6.6.3 Observing the timeline of an incident to give an accurate representation to interested parties including parents, children, and members of the public.
- 6.7 **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.**

6.8 The CCTV system is checked periodically by Mr P Archer to ensure that it is operating correctly.

## **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 30 days unless there is a specific purpose for which they are retained for a longer period.

7.3 Recorded images of incidents will be stored for a period of 6 calendar months for the purpose of assisting internal or law enforcement investigations.

7.4 SSPP 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:

7.4.1 CCTV recording systems being in restricted access areas.

7.4.2 The CCTV system being encrypted/password protected.

7.4.3 Restriction of the ability to make copies to specified members of staff.

7.5 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 SSPP.

## **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 [Trust's/School's] Subject Access Request Policy.

8.3 When such a request is made, Mr P Archer 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 member of staff handling the request 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 SSPP 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 staff member accessing footage 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 SSPP 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 from a law enforcement agency for disclosure of CCTV images, then Mr P Archer 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 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 - this record should be available to view in during the annual GDPR Audit.

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 every 2 years.

10.2 The CCTV system and the privacy impact assessment relating to it will be reviewed every 2 years.

## **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 SSPP should be made in accordance with SSPP Complaints Policy.

Date Reviewed	February 2023
Next Review Date	February 2025
Reviewer	Trust Audit & Risk Committee / OLoL Trust Exec Board / School
Author	Browne Jacobson template – edited by Tamer Robson & Will Ottowell & OLoL Schools



## CCTV PRIVACY IMPACT ASSESSMENT

1 Who will be captured on CCTV?

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

2 What personal data will be processed?

Facial Images, behaviour, and sound.

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

Deterrent for poor behaviour and damage to school property as well as Prevention and detection of crime.

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?

Mr P Archer

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) Cameras around site are located at regular intervals and placed such as to avoid blind spots in the coverage.
- b) Camera locations were chosen on the initial setup of the system. The locations have not been modified since as they fulfil coverage and location requirements.
- c) Only 1 Camera is placed in a location where it might capture footage of a third-party premise. The CCTV software has been used to block off the area, so it is not recorded.
- d) Signs indicating recording of CCTV are placed in a prominent position at the front of the school and in a place that can be seen when walking into school. The signs are bright yellow and describe the 24/7 recording nature of the system.
- e) The system does not support redaction of individual faces.

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

No sharing of the CCTV is done by default.

All requests for CCTV images (Including from law enforcement) must go through the SAR process.

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

30 days of live footage.

Specific recorded footage of incidents is kept for 6 calendar months to assist with internal and law enforcement investigations.

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

CCTV Recording Systems are password protected.

Recordings of Incidents will be securely stored in the Academy's Microsoft Teams storage which is restricted to access by staff only with permission as per section 6 of the policy.

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

Potential data breach.  
Transfer of images to third party.

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

Data systems are robust as possible, not previously been victim to this. No data will be transferred to third parties except for law enforcement agencies.

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?

NA - System has been installed for a long period of time already so there is a reasonable expectation that parents and children are aware of the system. The CCTV policy is available publicly on the academy website.

13 When will this privacy impact assessment be

reviewed? Every 2 years

**Approval:**

This assessment was approved by the Data Protection Officer:

DPO \_\_\_\_\_

Date \_\_\_\_\_