ST PETER'S COLLEGE
UNIVERSITY OF OXFORD

CCTV Policy, Standards and Procedures

Policy

St Peter's College seeks to ensure, as far as reasonably practical, the security and safety of all fellows, students, staff, visitors, guests, contractors and property, while within and around College premises. To this end CCTV cameras are deployed at various locations within and around the College estate, to assist in the prevention and detection of crime, or infringements of the College's regulations, the welfare and safeguarding of students and the safety of those on college premises.

Document purpose

This document details the operating standards and procedures for closed circuit television (CCTV) systems installed at St Peter's College, Oxford, in accordance with the requirements of:

- The Data Protection Act 2018 (DPA).
- The General Data Protection Regulation 2018 (GDPR).
- The Surveillance Camera Code of Practice, as updated in November 2021 issued by the Biometrics and Surveillance Camera Commissioner: https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version
- Article 8 of the Human Rights Act Right 1998. Respect for Private and Family Life.

Operating Principles

To ensure compliance with the legislation listed above, all CCTV operations, must at all times, adhere to the following principles.

- Fairly and lawfully processed.
- Processed for limited purpose and NOT in any manner incompatible with the purpose of the system.
- Adequate, relevant and not excessive.
- Accurate.
- Images are not retained for longer than is justifiably necessary.
- Processed in accordance with the individual's rights.
- Secure.

Operational Management

The operational management of the CCTV is the responsibility of the Head Porter.

Data and Privacy Protection

Responsible Persons

The College Responsible Person for data privacy/security matters is the Bursar. The external Data Protection Officer, registered with the Information Commissioner's Office (ICO) is GCRI Law Ltd.

The College Responsible Person for CCTV is the Bursar, Simon Jones

- The Bursar is the final decision-making authority as regards requests under the terms of the Freedom of Information Act and requests from Data Subjects (persons whose images have been recorded by the system).

Other responsible College personnel:

(a) Head Porter: Derrick Harriott

(b) Domestic Bursar: Kevin Melbourne

(c) IT Manager: Simon Thomson

- Responsibilities for safeguarding the data, preventing unauthorised access and compliance with the operating principles.

CCTV Control of Viewing and Access to Data

All viewing of the CCTV images will be carried out in the lodge. No unauthorised access to the CCTV screens will be permitted at any time. Access will be strictly limited to the duty porter(s) and the Responsible Persons noted above. Images saving to other formats such as USB Memory Sticks will only be carried out using the computer on the Head Porter's desk or in the IT office.

The library operates a single camera to prevent and investigate book theft. Library staff are only able to view images from this single camera and it is therefore out of the main CCTV system but must be managed in line with the policy outlined in this document.

CCTV viewing or observing in other places will only take place if authorised by a authorised Responsible Person. This includes remote viewing.

All staff working in the viewing area (lodge) will be made aware of the sensitivity of handling CCTV images and recordings. The Head Porter will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV.

Contractors working on the system will sign an undertaking that they understand and will comply with St Peter's College, CCTV Policy Standards and Procedures.

Subject to the appropriate Data Protection Act/GDPR written request (usually in the form of a data subject access request or 'DSAR') images are normally copied to a disc, which is then given to the requesting organisation or individual. In order to carry out this process, images are initially copied to a secure drive within the college system. Should there be any further requests, or if there has been a technical issue, these images are retained for two months on a secure password protected server. After two months these images are deleted by the Head Porter.

Access to/Disclosure of CCTV images

Access or disclosure requests such as DSARs must be authorised by a Responsible Person.

Third party requests for access to, or disclosure of (i.e. provision of a copy), images recorded on the College CCTV systems, will only be granted if the requestor falls within the following categories.

1. Data subjects (persons whose images have been recorded by the CCTV systems) where a data subject access request has been made and the relevant Responsible Person has agreed to the disclosure.
2. Law enforcement agencies with the appropriate legal instrument, such as a Court Order, covering the specific information/footage requested.
3. An authorised college member who has responsibility for student discipline
4. An authorised college member who has responsibility for welfare and safeguarding of students
5. An authorised member of college staff in the investigation of a Health and Safety at Work Act incident.
6. An authorised member of staff in the investigation of crime.
7. Relevant legal representatives of data subjects.
8. An authorised member of College staff in the investigation of staff disciplinary issues.

The Bursar will be responsible for granting the authorisations noted above or, in their absence (Domestic Bursar

Access to images by a law enforcement agency

Law enforcement agencies may view or request copies of CCTV images subject to providing an appropriate legal instrument, such as a warrant or Court Order and in accordance with the protocols contained within this document. In very urgent serious cases of crime or public safety, relevant law enforcement agencies may view CCTV images if requested in person and subject to authorisation by one of the Responsible Persons.

Access to images by a subject

CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act and the GDPR. Anyone who believes that they have been filmed by CCTV is entitled to ask for a copy of the data, subject to exemptions contained in the Act, notably where the images show other individuals in

addition to the data subject (such third-party data would need to be redacted in most cases). They do not have the right of instant access.

A person whose image has been recorded and retained and who wishes access to the data must apply in writing to a Responsible Person using a CCTV Subject Access Request form. Subject Access Request Forms are obtainable from the lodge (As at Appendix 'B').

All applications must be made by the Data subject themselves, or their legal representative.

The Data Protection Act and the GDPR give the College the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, or the images have been erased. If a data subject access request is refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

Rights in relation to Automated Decision Taking

St Peter's College CCTV system is not used in any manner in relation to automated decision taking.

System Description

Any changes or additions to the system will be in compliance with the Data Protection Act, the GDPR and the Surveillance Commissioners CCTV Code of Practice.

St Peter's College CCTV has a number of IP cameras on three sites with images being transmitted to a secure server for storage and for recall at a later date, with a live feed being streamed from the server to the Lodge monitors on the main site.

The system comprises: Fixed position cameras and a single pan and tilt camera; Monitors: Multiplexers; Digital recorders; Information signs.

Cameras are located at strategic points on the six sites, principally at the entrance and exit point of sites and buildings. No cameras are hidden from view and none cover any areas which would be considered private. The college system does not have covert cameras.

The system is NOT capable of recording audio.

There are signs prominently placed at strategic points and at entrance/exit points informing that a CCTV installation is in use.

System log on is by individual or authorised department, the server is separately password protected. CCTV images are retained for up to 28 days, after this period the system automatically overwrites the existing data on a rolling basis. Images burned off for enforcement and investigation are kept for three months on a secure server then deleted by the Head Porter, once that period has reached. This is to ensure a backup should there be an issue with images burned to a CD.

The sites on which CCTV is used are:

St Peter's College Main site New Inn Hall Street Oxford OX1 2DL
Paradise Street Oxford OX1 1LD
Lau Building Oxford OX1 1NG
St Thomas Street Oxford OX1 1HQ
Castle Bailey Quad New Street Oxford
Barron House New Road Oxford

Policy and Procedures Review

Review date: September 2025

Appendix A: CCTV Privacy Impact Assessment

This Privacy Impact Assessment (PIA) CCTV is recommended in The Surveillance Camera Code of Practice, issued by the Surveillance Camera Commissioner and updated in January 2022 in accordance with Section 30 (1) (a) of The Protection of Freedom Act 2012. The purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the CCTV to be met whenever possible.

Document Purpose

The purpose of this Privacy Impact Assessment is to ensure that the use of a surveillance camera system must consider its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

The Surveillance Commissioner's Code of practice identifies 'the need for a privacy impact assessment process to be undertaken whenever review of a surveillance camera system is being considered to ensure that the purpose of the system remains justifiable, there is consultation with those most likely to be affected, and the impact on their privacy is assessed and any appropriate safeguards can be put in place.

A privacy impact assessment also helps assure compliance with obligations under the Human Rights Act 1998 which specifies that; everyone has the right to respect for their private and family life, their home and their correspondence.

Compliance Measures

See St Peter's College CCTV policy

System/Cameras

See CCTV Policy- in particular Appendix 'A' Camera Operational Requirement

Each camera has its own individual assessment of operational requirements, detailing the justification for its installation, location and the extent of what it views. Although this particular document is confidential, should a person express a need to view the information relating to an individual camera, the relevant section of the document relating to this camera can be shown to this person in a controlled environment.

All cameras are deployed solely for the reasons of the prevention and detection of crime, or public safety.

There are no cameras which view student's rooms, kitchens or accommodation corridors.

There are no cameras within student accommodation. Any cameras on which student's windows can be seen, have the window areas blocked out on the monitor and on playback.

No cameras are hidden from view and none cover any areas which would be considered private. The college does not have any covert cameras.

Cameras are only used by trained operatives and the range of features available from a camera are utilised by an Operator when patrolling a camera or responding to an incident. An Operator may zoom in to capture an identifiable image of an individual. This would be to assess whether behaviour is suspicious, to identify if they are the suspect or victim of a crime or whether they match an identity as described in information supplied from an authorised source, such as OUSS or Police intelligence information.

All viewing and observing of the CCTV images is carried out in the lodge. No unauthorised access to the CCTV screens is permitted at any time. Access is strictly limited to the duty porter (s), or the Responsible Persons.

All access to the CCTV system is via an individual password, this includes the servers.

The system does not have facial recognition software.

None of the system cameras have audio.

There is legally compliant signage at appropriate areas of the college.

The monitors can only by viewed by authorised persons (Lodge Staff).

The monitors are in a restricted access area and cannot be viewed by the public.

All users have been given CCTV training, particularly covering appropriate usage and legal aspects of CCTV.

The library operates a single camera to prevent and investigate book theft. Library staff are only able to view images from this single camera. Library staff has received the same CCTV training as lodge team members.

Appendix B: St Peter's College CCTV Subject Access Request Form

The Data Protection Act (DPA) and the GDPR provide Data Subjects (individuals to whom "personal data" relates) with a right to access personal data held about themselves, including images recorded on closed circuit television (CCTV) systems.

To enable St Peter's College to deal promptly with your request for access to the CCTV images, please complete the form giving as much information as possible to help us identify your personal data.

Under the terms of the DPA, the College must respond within one calendar month to process your request; however, the college will endeavour to respond within a shorter time period. This time period will ordinarily commence on the date that the completed form, or other communicated request, containing sufficient information to enable the St Peter's College to locate the relevant images.

Please note the Data Protection Act/GDPR may provide grounds to refuse or limit the request.

Please also note that the Freedom of Information Act may provide exemptions to complying with this request.

(Please use BLOCK CAPITALS to complete this form)

1. Data Subject Personal details

Title.	First Name	Surname

Address
Telephone Number
Email address

If the application is by a third party please state name address, relationship to the Data Subject and reason for the application. Please note we will contact the Data Subject to confirm relationship.

Title	First Name	Surname

Address
Telephone Number
Email address
Relationship to Data Subject
Reason for application

2. Information Required to Locate Images

In order for the Data Controller to identify the images you require access to, please provide the following information:

The exact date(s) and location(s) of the CCTV camera(s) which captured the footage required and approximate time:

Date
Time
Location (s)

Please give sufficient personal characteristics to enable identification of the Data Subject (a full description including hair colour, clothing etc.). Please use a separate sheet of paper if necessary. If you are not a member of the college it would help if you supplied a photograph.

3. Access to Images

Assuming the Data Controller is able to locate the required images, please select which of the following will satisfy your request.

I would like to view the relevant images at the College.	
I would like to be sent a copy of the relevant images.	

I acknowledge that it may be necessary for the Data Controller to contact me to obtain further information to satisfy my identity or to locate my personal data.

Name	Signature	Date

Please return this form to the Bursar in a sealed envelope. If an online form please email it to bursar@spc.ox.ac.uk