



ST. HUGH'S COLLEGE, OXFORD

CCTV Code of Practice

Date Policy Ratified by Governing Body: 20 May 2026

Committee Responsible: Finance and General Purposes Committee

Date to be reviewed by: 20 May 2028

St Hugh's College CCTV Code of Practice

In order to fulfil educational, pastoral, administrative and employment responsibilities the College needs to collect and process personal data, including about students, staff, alumni, and the general public. For security reasons we monitor key areas of the site using CCTV and retain recordings of CCTV footage as set out in this Code of Practice.

CCTV viewing is classed as information and any CCTV product is classed as Data under the Data Protection Act 1998 and the College has a legal obligation to comply with the law. Information must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

This code has been adopted in order to:

- Ensure compliance with the law and ICO guidance;
- Gain public trust by ensuring that legally required safeguards are in place and complied with;
- Protect individuals when their data is processed;
- Enable data sharing when this is necessary and beneficial;
- Create trust and a better relationship with the people whose Information the College needs to process;
- Reduce the risk of inappropriate or insecure sharing of personal data;
- Ensure a common understanding of when, or whether, it is acceptable to share information without people's knowledge or consent or in the face of objection; and
- Reduce risk of questions, complaints and disputes about the way the College shares personal data.

CCTV System objective

The objective of the St Hugh's College CCTV system is to enhance the security and safety of everyone on the College site, including the prevention and detection of unacceptable behaviour and crime.

Document Purpose

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

- General Data Protection Regulations 2018
- Freedoms of Information Act 2012
- The Home Office CCTV Code of Practice 2013
- ICO data protection code of practice for CCTV and personal information 2014
- Article 8 of the Human Rights Act 1998. Respect for Private and Family Life.

Data Protection Principles

As the data controller for the CCTV System, the College is obliged to comply with the data protection principles embodied in the General Data Protection Regulations.

The 7 key principles are:

1. Lawfulness, fairness and transparency

St Hugh's College meets this requirement achieving voluntary certification with the Surveillance Camera Commissioners Codes of Practice and has published the following documents:

- CCTV Code of Practice
- Privacy Notice
- Data Protection Impact Assessment (formerly PIA)
- CCTV warning signs are clearly displayed to indicate the presence of CCTV
- Annual systems audit to ensure there is a legitimate reason and pressing needs for cameras continued deployment

2. Purpose limitation
St Hugh's College meets this requirement by publishing a Privacy Notice; defining objectives for the CCTV System in this policy; carrying out periodic audits (GDPR Audit carried out by Lodge Manager annually next review Nov 2026); and reviewing the continued justification for deploying individual cameras in relation to the objectives.
3. Data minimisation
St Hugh's College meets this requirement by ensuring that the routine retention of recorded material does not exceed 30 days.
4. Accuracy
St Hugh's College meets this requirement by ensuring through regular maintenance that the CCTV System is capable of producing images of sufficient quality to be admitted as evidence in legal proceedings.
5. Storage limitation
St Hugh's College meets this requirement by ensuring that the routine retention of recorded material does not exceed 30 days.
6. Integrity and confidentiality (security)
St Hugh's College meets this requirement by formulating and implementing appropriate technical and organisational policies and procedures.
7. Accountability
St Hugh's College meets this requirement via its Data Protection Policy, ROPRs, and the publication of key documents including this policy.

Human Rights Act 1998

St Hugh's College recognises that relevant authorities and those organisations carrying out the functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998 and considers that the use of CCTV across the College is necessary, addressing a legitimate aim and pressing need; being a proportionate and suitable tool to help prevent and detect unacceptable behaviour and crime, reduce concern from College members, and improve safety. This is supported by the use of 'operational requirement' documents which relate to all cameras on the system outlining the justification for their deployment.

St Hugh's College's CCTV System will be operated with respect for all individuals. It is recognised that the operation of the CCTV System may be considered to infringe on the privacy of individuals. The college recognises that it has a responsibility to ensure that the scheme will only be used as a proportionate response to identified problems and be used only in so far as it is necessary to support the system's objectives.

Operating Principles

To ensure compliance with the 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 individuals' rights
- Secure

1. Operational Management

The operational management of the CCTV is the responsibility of the Lodge Manager or their Deputy.

CCTV Operators

All CCTV operators and authorised staff, including managers, must receive training relevant to their role in relation to the General Data Protection Regulations, Human Rights Act and the Protection of Freedoms Act – Surveillance Camera Commissioner’s Codes of Practice. Operators’ training will be subject to periodic audit. CCTV operators are not required to be SIA licensed because they are employed directly by St Hugh’s College. Breaches of this policy or of local or legal operating requirements by a CCTV operator may be liable to disciplinary action.

2. Data and Privacy Protection

Responsible Persons

The College Data Protection Officer is the College Secretary. The Responsible Officers for the CCTV system and any product deriving from it are the Bursar and the Lodge Manager. The Bursar has the final decision-making authority as regards requests for CCTV data for operational purposes, including for disciplinary or other reasons. Standing approval may be given for particular categories of urgent incident. In addition, the Lodge Manager has delegated authority regarding urgent requests for CCTV data from law enforcement or the emergency services.

Data Controller

The Data Controller is the Lodge Manager, who is responsible for safeguarding the data, preventing unauthorised access and compliance with the operating principles.

3. CCTV Control of Viewing and Access to Data

All viewing and observing of the CCTV images will be carried out in the Lodge Manager’s office. 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 Data Protection Officer. Image saving to other formats such as DVD discs, will only be carried out using the Lodge Manager’s computer terminal. CCTV viewing or observing in other places will only take place if authorised by the Data Protection Officer or the Bursar. This includes remote viewing.

Any staff member working in these areas should:

- a. Sign the ‘Declaration of Code of Practice for the operation of St Hugh’s College CCTV’ (Held by Lodge Manager – see section 9)
- b. Ensure that details of any event witnessed by a staff member via live footage may only be revealed to other staff members if this information is required for the “strict performance of their duties”- this should permit staff to pass on important information seen on the live footage and ensure disclosure only when there is an operational need to do so.

All staff working in the viewing area (Lodge) will be made aware of the sensitivity of handling CCTV images and recordings. The Lodge Manager will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV. Images are retained on a secure hard drive for up to 28 days; after this period, they are automatically overwritten.

The ability to review recorded CCTV footage requires each user to input the password. Each member of staff will be responsible for any usage of the system by them whilst on duty (Lodge log in). Before any use of the system the user must:

- a. Have read and understood the UK Government's 'Surveillance Camera Code of Practice' dated June 2013
- b. Signed the 'Declaration of Code of Practice for the St Hugh's College CCTV Operators'
- c. Ensure that all requests to show / review or produce and distribute any recorded footage must be authorised in writing by the Lodge Manager, the Data Protection Officer on the 'CCTV Request Form' (see attachment 2) designed for this purpose.

Subject to the appropriate Data Protection Act provisions, images authorised to be shared are normally copied, the copy then being 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 Lodge Manager.

4. Access to/Disclosure of CCTV images

Access or disclosure requests will only be authorised by the Bursar or Lodge Manager

Requests for access to, or disclosure of (i.e. provision of a copy), images recorded on the College CCTV systems from third parties, 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).
2. Law enforcement agencies.
3. An authorised college member who has responsibility for student welfare or discipline - in the course of a student investigation.
4. An authorised member of college staff in the investigation of a Health and Safety at Work Act incident.
5. An authorised member of staff carrying out an investigation under one of the College's employee procedures (e.g. disciplinary, grievance).
6. Relevant legal representatives of data subjects.
7. Other individuals as authorised in writing by the Bursar.
8. Other individuals when required for legal or regulatory compliance.

5. Access to images by a law enforcement agency

Law enforcement agencies may view or request copies of CCTV images subject to providing an appropriate written Data Protection Act 1998 request 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 verbal authorisation by the Lodge Manager, Bursar, Principal, DPO, or most senior officer on duty. Subsequent written authority is to be approved by the Data Protection Officer, if the request by law enforcement agencies to view or copy CCTV is urgent and operationally necessary.

A college pro-forma is used for this purpose and all written requests and all written refusal of requests are filed with the Data Protection Officer.

In the event of an incident where the police or University Proctors Officers request to review or have a copy made of St Hugh's College CCTV footage, the following procedure should be applied:

- a. No action should be taken by any member of St Hugh's College's CCTV operators that frustrates or delays Police enquires and prevents or obstructs their investigation. CCTV operators should comply with all reasonable requests made of them by the Police or other agencies.

- b. Reasonable requests to review CCTV made by the Police in the course of their investigations must be authorized by Lodge Manager or Bursar by email.
- c. The copy is to be given a recognisable exhibit name by the person producing the copy and the whereabouts of that copy are to be monitored with a written audit trail and destroyed when no longer necessary to retain it.
- d. The party requesting to view CCTV images or have a copy produced must complete the 'CCTV Request Form' in conjunction with the staff member facilitating the viewing or producing any subsequent material. This can be done in the absence of the Bursar or Lodge Manager and should not delay the Police or Proctors Officers in obtaining the information or product they require. Ideally the Bursar or Lodge Manager should be informed verbally of the Police or Proctors requests.
- e. If the request is declined, it is for the Bursar to explain to the requesting party or representative why the request has been declined. A written and signed record using the pro-forma is to be retained documenting the refusal and reason(s).
- f. All completed CCTV request forms should be filed with the Data Protection Officer.

6. Access to images by an individual subject

CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act. 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. They do not have the right of instant access. Additionally, persons may make a Freedom of Information Act request. Data Subject Access Requests and Freedom of Information Act requests are handled under the appropriate college policies and procedures.

7. System Description

Any changes or additions to the system will be in compliance with the Data Protection Act and the Information Commissioner's Office CCTV code of practice.

St Hugh's College CCTV has a number of IP cameras on site 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 Lodge Manager can access CCTV via a password which leaves an auditable trail. The system comprises: Fixed position cameras; Monitors: Multiplexers; Digital recorders; Information signs.

Cameras are located at strategic points on the main College grounds, principally at the entrance and exit point of sites and buildings. 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 an authorised account, the server is separately password protected. CCTV images are retained for up to 30 days, after this period the system automatically overwrites the existing data on a rolling basis.

8. System Registration

St Hugh's College CCTV system is registered with the Information Commissioners Office- Data Protection Register.

The existence of this policy and information on access and applications for copies of CCTV data should be referenced in the St Hugh's College Student and Staff handbooks. A separate document

(Appendix to this Code of Practice) will be produced which details the operational requirement of each CCTV camera, justifying its position and providing a snap-shot of the camera view.

All additions or alterations to the current CCTV camera equipment must be authorised by the Data Protection Officer (College Secretary) and the relevant Appendix amendments made by the Data controller.

9. Review

CCTV Code of Practice / Policy and Procedures:

- Consistent with ICO guidelines
- To be reviewed annually - Next Review due: October 2026
- GDPR Audit carried out by Lodge Manager annually next review Feb 2026.
- CCTV Operators Sign the 'Declaration of Code of Practice for the operation of St Hugh's
- College CCTV (Next Review, Oct 2026)
- Privacy Notice (Next Review, Oct 2026)