Oriel College
UNIVERSITY OF OXFORD

CCTV CODE OF PRACTICE

Version: v.6
Approved by House Committee: 6 February 2026
Approved by Governing Body: 11 February 2026
Next review date: Hilary Term 2027

CONTENTS

A. Introduction

The legitimate objective of the Oriel College CCTV system is the prevention and detection of crime, and maintaining a safe and secure environment for staff, students, and visitors. We recognise that this may raise concerns about the effect on individuals and their privacy. This Code of Practice ("the Code") is intended to address such concerns.

Images recorded by CCTV are personal data which must be processed in accordance with data protection laws. We are committed to complying with our legal obligations and ensuring that the legal rights of staff, students, and visitors, relating to their personal data, are recognised and respected.

Human Rights Act 1998

Oriel 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 consider 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 a crime, reduce fear of crime and improve public 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.

Oriel College's CCTV 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.

B. Information Security Classification

This Code will be published on the College's website for the information of College members and visitors, and to demonstrate the College's robust stance on data protection. The code will also be available on the College's internal SharePoint resource, and will be available from the Governance Officer (governance@oriel.ox.ac.uk) on request.

C. Delegated Authority

The Domestic Bursar has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this code.

The code will be overseen by the House Committee who will review recommendations made by the Domestic Bursar to ensure that the code is continually compliant with changes in Data Protection (GDPR) legislation. This code will be reviewed annually alongside the College's data protection policies.

Day-to-day operational management of the CCTV and the storage of data recorded is the responsibility of the Lodge Manager or their Deputies. Day-to-day management responsibility for deciding what information is recorded, how it will be used, and to whom it may be disclosed has been delegated to the Lodge Manager, supported by the Domestic Bursar. The Lodge Manager and their Deputies can rewind CCTV when necessary, but decisions on downloading CCTV rests with the Domestic Bursar. The Lodge Manager and their Deputies are the College's designated 'Security Industry Authority' (SIA) CCTV Operators.

The Governance Officer will ensure that this code is updated in line with all approved reviews and amendments suggested by the House Committee and approved by the Governing Body.

D. Policy Statement

This Code has been adopted for the reasons outlined below. We believe that such use is necessary for legitimate business purposes, including:

- To prevent crime and protect buildings and assets from damage, disruption, vandalism, and other crime.
- For the personal safety and welfare of staff, students, visitors, and other members of the public, where there is a reasonable concern for their safety or wellbeing, and to act as a deterrent against crime.
- To support law enforcement bodies in the prevention, detection and prosecution of crime.
- To assist in day-to-day management, including ensuring the health and safety of staff, students, and others.
- To assist in the effective resolution of disputes which arise in the course of staff disciplinary or grievance proceedings.
- To assist in the effective resolution of disputes which arise in the course of student disciplinary or grievance proceedings

- To gain public trust by ensuring that legally required safeguards are in place and complied with.
- To reduce reputational risk caused by the inappropriate or insecure sharing of personal data.
- To achieve a better understanding of when, or whether, it is acceptable to share information without people's knowledge or consent, or in the face of objection.
- To reduce risk of questions, complaints, and disputes about the way the College shares personal data.

This list is not exhaustive and other purposes may be, or may become, relevant.

E. Definition of Terms

For the purposes of this Code, the following terms are defined as such:

"CCTV"
Means fixed and domed cameras designed to capture and record images of individuals and property and for the purpose of this Code, may include any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes any technology that may be introduced in the future such as automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

"Data"
Is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

"Data subjects"
Means all living individuals about whom we hold personal information as a result of the operation of our CCTV.

"Personal Data"
Means our data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

"Data controllers"
Are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law.

"Data users"
Are those of our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this Code and our GDPR Data Protection Policy.

"Data Processors"
Are any person or organisation that is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

"Processing"
Is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending retrieving, using, disclosing, or destroying it. Processing also includes transferring personal data to third parties.

F. Procedure

Use of CCTV
We currently use CCTV to view and record individuals on (and around) our premises. This Code details how we will use CCTV and how we will process data recorded by CCTV cameras to ensure we are compliant with data protection law and best practice. This Code also explains how to make a subject access request in respect of personal data created by CCTV.

We recognise that information that we hold about individuals is subject to data protection legislation. The images of individuals recorded by CCTV are personal data and therefore subject to data protection legislation. We are committed to complying with all our legal obligations and seek to comply with best practice suggestions from the Information Commissioner's Office (ICO).

CCTV Monitoring and Operating
Oriel College has a number of CCTV cameras on its premises. Cameras are located at strategic points on the main College

grounds, island site, and Rectory Road site and Oriel college sports ground, principally at the entrance and exist point of sites and buildings.

The CCTV use is 24 hours a day and this data is continuously recorded. The CCTV is NOT capable of recording audio.

CCTV locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. As far as practically possible, CCTV will not focus on private homes, gardens, or other areas of private property.

There are signs prominently placed at strategic points and at entrance/exit points informing that a CCTV is in use and that individuals' images may be recorded. Such signs will contain details of the organisation operating the CCTV, the purpose for using the CCTV and who to contact for further information, where these things are not obvious to those being monitored.

Images are monitored by authorised personnel 24 hours a day every day of the year.

Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety. We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose work requires them to have access to such data. Recorded images will only be viewed in designated, secure offices.

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:

a) Data subjects (persons whose images have been recorded by the CCTV systems).
b) Law enforcement agencies.
c) The Senior Dean who has responsibility for student welfare and discipline, where access is necessary in the course of a student investigation, or in response to a specific and reasonable student welfare or safeguarding concern.
d) Lodge manager in the investigation of a Health and Safety at Work Act incident.
e) Lodge Manger in the investigation of crime.
f) The College Librarian, where access is necessary and proportionate in response to a legitimate and specific concern relating to the site security of the Library premises.

g) Relevant legal representatives of data subjects.
h) Other staff requests must come from either the domestic Bursar or Treasurer

The CCTV system comprises:

- Fixed position cameras.
- Monitors.
- Multiplexers.
- Digital Recorders.
- Information signs.

Use of Data gathered by CCTV

In order to ensure that the rights of individuals recorded by the CCTV are protected, we will ensure that data gathered from CCTV is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.

Given the large amount of data generated, we may store footage using DVD disks, memory sticks and/or cloud computing systems. We will take all reasonable steps to ensure that any cloud service provider maintains the security of our information, in accordance with industry standards.

We may engage data processors to process data on our behalf. We will ensure reasonable contractual safeguards are in place to protect the security and integrity of the data.

Retention and erasure of data gathered by CCTV

Data recorded by the CCTV will be stored on a secure hard drive. Data from CCTV will not be retained indefinitely, but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded.

For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to be resolved. In all other cases, recorded images will be kept for up to 28 days; after this period, they are permanently deleted. We will maintain a comprehensive log of when data is deleted.

At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as DVDs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

Use of Additional Surveillance Systems

Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully

consider if they are appropriate by carrying out a Data Protection Impact Assessment (DPIA).

A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances. A DPIA will consider the nature of the issue being addressed, identify any risks to individuals and their rights, and determine what measures and safeguards are required to mitigate those risks and ensure protection of personal data and compliance with data protection legislation.

No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

Covert Monitoring

We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of the Domestic Bursar. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent workers and/or students will always be a primary consideration in reaching any such decision.

Only limited numbers of people will be involved in any covert monitoring.

Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

Disclosure of CCTV Images

No images from our CCTV will be disclosed to any third party without express authorisation from the Data Protection Officer (the Treasurer). Data will not normally be released unless satisfactory

evidence that it is required for legal proceedings or a court order has been produced.

In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

We will maintain a record of all disclosures of CCTV footage.

Access to Images by an Individual Data Subject

Under the data protection legislation, data subjects may make a request for disclosure of their personal information and this may include CCTV images. This is known as a "data subject access request." A data subject access request is subject to the statutory conditions from time to time in place and should be made in writing.

You will not have to pay a fee. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances of unfounded, repetitive, or excessive requests.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

We may also contact you to ask you for further information in relation to your request to speed up our response.

In order for us to locate relevant footage, any requests must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

We try to respond to all legitimate requests within one calendar month. Occasionally, it could take us longer if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

We reserve the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, where we consider it necessary to do so.

Requests under the Freedom of Information Act (FOIA) 2000.

Individuals may make a Freedom of Information request and we shall respond to such requests within 20 working days of our receipt of such a request. Occasionally it could take us longer than 20 working days if your request is particularly complex, you have submitted a number of requests, or if your request requires a public interest test.

Freedom of information requests relating to footage captured by College CCTV should be sent to the FOI officer (foi@oriel.ox.ac.uk) and include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual. We may in certain circumstances charge an administrative fee for processing such a request.

The FOIA 2000 gives the Freedom of Information Officer exemptions under Section 40 and 38 of the Act, which would prevent disclosure of CCTV images. If a refusal is made under these exemptions, the reasons will be fully documented in and the Data Subject informed in writing, stating the reasons. A college pro-forma is used for this purpose and all requests and responses are filed with the Treasurer's Office under the oversight of the Freedom of Information Officer and Data Protection Officer (the Treasurer).

G. Scope

This code covers all employees, directors, officers, consultants, contractors, freelancers, students, volunteers, interns, agency workers and visiting members of the public.

H. Training and Responsibilities

All staff responsibilities in relation to the successful operation of this code are set out in **section C** above.

All CCTV operators and authorised staff have received training relevant to their role to ensure that they understand and observe the legal requirements related to the processing of relevant data and relevant legislation. Operators' training will be subject to an annual audit.

I. Internal Help and Raising Concerns

Complaints and More Information

For more information, our Privacy Notice can be found on our website, or provided upon a request made to the Governance Officer (governance@oriel.ox.ac.uk).

If you have any questions or complaints about this code or any concerns about our use of CCTV, please contact the Treasurer or Domestic Bursar (treasurer@oriel.ox.ac.uk).

Requests to Prevent Processing

We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making.

For further information, please see Articles 21 and 22 of the General Data Protection Regulation, or contact the Data Protection Officer (foi@oriel.ox.ac.uk).

J. Consequences of Non-Observance

A breach of this code may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this Code may be regarded as misconduct leading to disciplinary action, up to an including dismissal.

K. Further Help

Further questions regarding this policy should be directed to the Treasurer or Domestic Bursar.

L. Reference

This policy should be read in conjunction with the College's Data Protection Policy.

M. Policy Version Control Table

Version	Owner	Agreed by House Committee	Agreed by Governing Body	Reason for amendment	Amended by	Next review	Further notes
v.1	Lodge Manager	1 June 2016	15 June 2016	This is the original version.			GB approval was subject to student approval which was achieved on 19.10.2016 at a meeting of the House Committee when JCR and MCR student representatives approved the policy.
v.2	Lodge Manager	17 October 2018	7 November 2018	Scheduled review.	Lodge Manager		
v.3	Lodge Manager	27 January 2021	10 February 2021	Scheduled review.	Lodge Manager		
v.4	Lodge Manager	18 October 2023	8 November 2023	Scheduled review.	Lodge Manager		
v.5	Domestic Bursar	7 February 2025	12 February 2025	Scheduled review	Lodge Manager and Domestic Busar	**HT26**	
v.6	Domestic Bursar	Approved via circulation on 6th February 2026	11 February 2026	Scheduled review.	Governance Officer; Lodge Manager; Domestic Bursar	**HT27**	

N. Appendices

Registration

Oriel College CCTV is registered with the Information Commissioners Office's (ICO) Data Protection Register. Registration number: Z1722079.

For the document detailing the operational requirements of each CCTV camera, justifying positioning and providing a snap-shot of the camera view, please contact the Governance Officer (governance@oriel.ox.ac.uk).