Oriel College CCTV Code of Practice

In order to fulfil educational, pastoral, administrative and employment responsibilities the College needs to collect and process personal data about students and staff.

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:

- Minimise the risk of breaking the law and consequent enforcement action by the ICO or other regulators;
- Gain public trust by ensuring that legally required safeguards are in place and complied with;
- Protect individuals when their data is shared;
- Enable data sharing when this is necessary and beneficial;
- Create trust and a better relationship with the people whose Information the College needs to share;
- Reduce reputational risk caused by the inappropriate or insecure sharing of personal data;
- 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; and
- Reduce risk of questions, complaints and disputes about the way the College shares personal data.

1. Document Purpose

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

- The Data Protection Act 1998 (DPA).
- The Home Office CCTV Code of Practice 2013 issued by the Information Commissioners Office (ICO).

- ICO data protection code of practice for CCTV and personal information 2014
- Article 8 of the Human Rights Act Right 1998. Respect for Private and Family Life.

2. 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.

3. Operational Management

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

4. Data and Privacy Protection

Responsible Persons

The College Data Protection Officer is the Treasurer. The Data Protection Officers for the CCTV system and any product deriving from it are the Lodge Manager.

- The Lodge Manger has the final decision making authority as regards requests under the terms of the Freedom of Information Act for CCTV data, and requests from Data Subjects (persons whose images have been recorded by the system).
- The Senior Dean has the final decision making authority as regards requests for Decanal or Welfare reasons.

Data Controller

The Data Controllers are the Lodge Manager and Deans.

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

5. CCTV Control of Viewing and Access to Data

All viewing and observing of the CCTV images will be carried out in the Lodge or the terminal at Rectory Road. No unauthorised access to the CCTV screens will be permitted at any time. Access will be strictly limited to the duty porter(s), Deans and the Data Protection Officers. Image saving to other formats such as DVD discs, will only be carried out using the Lodge Manager's computer terminal or a terminal authorised by the Senior Dean. CCTV viewing or observing in other places will only take place if authorised by the Data Protection Officers. This includes remote viewing.

Any staff member working in these areas should:

a. Sign the 'Declaration of Code of Practice for the operation of Oriel College CCTV ' (see attachment 1)

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 over written.

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 Oriel 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, Deans and/or the Data Protection Officer on the 'CCTV Request Form' (see attachment 2) designed for this purpose.

Subject to the appropriate Data Act written request images are normally copied, 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 Lodge Manager.

6. Access to/Disclosure of CCTV images

Access or disclosure requests will only be authorised by the Data Protection Officer or a Data Controller.

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 (College HOD) in the investigation of crime.
6. Relevant legal representatives of data subjects.

7. 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 Data Controller or a Data Protection Officer. Subsequent written authority is to be approved by the Data Protection Officer (Domestic Bursar), 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 Lodge Manger.

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

a. No action should be taken by any member of Oriel 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. CCTV Operators should comply with all reasonable requests to review CCTV made by the Police in the course of their investigations.

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 Domestic Bursar or Lodge Manager and should not delay the Police or Proctors Officers in obtaining the information or product they require. Ideally the Domestic Bursar or Lodge Manager should be informed verbally of the Police or Proctors requests.

e. If the request is declined, it is for the Domestic 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 Lodge Manger.

8. 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.

A person whose image has been recorded and retained and who wishes access to the data must apply in writing to a Data Protection Officer using a Subject Access Request form. Subject Access Request Forms are obtainable from the Lodge.

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

In accordance with Government guidelines a £10 search fee will be charged and is to be received by the College Bursary before data is supplied.

Such requests will be processed promptly and in the case of a Freedom of Information request responded to within 20 days. In the case of a Data Protection Request a copy will be provided within 40 days.

The Data Protection Act gives the Data Protection Officer 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.

The Freedom of Information Act 2000 gives the Data Protection Officer exemptions under Section 40 and 38 of that act which would prevent disclosure of CCTV images. If a refusal is made under these exemptions, the reasons will be fully documented and the Data Subject informed in writing, stating the reasons. A college pro-forma is used for this purpose and all written requests and all refusals of requests are filed with the Domestic Bursar.

In the event of an incident where an internal College Officer requests a review of recorded footage, the following procedure should be applied. If a physical copy of CCTV footage is requested then permission must be sought from the Bursar.

a. Requesting Party must be a College Officer / Line Manager

b. Requesting Party & Lodge Porter fill out the 'CCTV Request Form'

c. The request must be made to either the Lodge Manager or Domestic Bursar and the person making the request must have a reason allowable by the 'Surveillance Camera Code of Practice' (https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf). If it is unclear whether the request is allowable, the matter must be referred to the Domestic Bursar.

d. If the request is to be actioned, the Lodge Manager or Domestic Bursar will review the footage with the College Officer / Line Manager.

e. If the request is declined, the Bursar will explain to the requesting party or representative why the request has been declined.

f. No footage can be held /copied for storage outside of the CCTV's 28 day period footage retention without the consent of the Domestic Bursar.

g. 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 an audit trail and destroyed when no longer necessary to retain it.

h. All CCTV Request Forms to be filed with the Domestic Bursar.

9. System Description

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

Oriel 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, island site and Rectory Road site, 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 28 days, after this period the system automatically overwrites the existing data on a rolling basis.

10. System Registration

Oriel College CCTV system is registered with the Information Commissioners Office- Data Protection Register: registration number Z5635808

The existence of this policy and information on access and applications for copies of CCTV data should be referenced in the Oriel 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 (Domestic Bursar) and the relevant Appendix amendments made by the Data controller.

11. Review

CCTV Code of Practice / Policy and Procedures -

- Consistent with ICO guidelines updated December 15
- To be reviewed annually - Next Review due: December 2019