CCTV Policy

1. Purpose

1.1 This policy seeks to ensure that the Close Circuit Television (CCTV) system used at Keble College, Oxford, is operated in compliance with the law relating to data protection legislation and the Human Rights Act 1998 (including but not limited to article 8 – Respect for Private and Family Life), as well as guidance issued by the Information Commissioners Office.

1.2 For the purposes of this policy, the 'Owner' of the system is Keble College.

1.3 For the purposes of data protection legislation, the "Data Controller" is Keble College.

1.4 Keble College uses CCTV only where it is necessary in the pursuit of a legitimate aim, and only if it is proportionate to that aim – balancing, as far as possible, the objectives of the CCTV System against the need to safeguard individual rights.

2. Operating Principles

2.1 To ensure compliance with the above legislation, all personal data processed as part of the CCTV system will be processed in accordance with the principles (Article 5) of the UK GDPR.

2.2 Images of identifiable individuals will only be shared when necessary, with information being given instead, where possible. For example, if the sole purpose of accessing images is for identification, the image should not be shared. It should be noted that the principles of GDPR would apply to such information, as well as to images.

3. Objectives

The objectives of the CCTV system are:

3.1 To protect the College and its assets

3.2 To monitor the security of the sites and property thereon

3.3 To provide safety and security for College members and visitors

3.4 To assist with the prevention and detection of crime, public disorder and offences against people

3.5 To support the police in a bid to deter and detect crime, identify, apprehend and prosecute offenders

3.6 To prevent, investigate and detect disciplinary offences in accordance with the College's disciplinary procedure

3.7 To identify and discipline individuals who breach College policies

3.8 To assist in the management of parking of both cars and bicycles

4. Key Personnel

4.1 The College's Data Protection Officer (DPO) is responsible for monitoring internal compliance with data protection legislation, advising on the College's data protection obligations and acting as a point of contact for individuals and the ICO. The DPO can be contacted via email at data.protection@keble.ox.ac.uk.

4.2 The Domestic Bursar is the overall manager for this system and has overall responsibility for ensuring the implementation of this policy. He can be contacted via email at domestic.bursar@keble.ox.ac.uk.

4.3 The IT Manager provides day-to-day support for the CCTV system.

4.4 The Lodge Manager and Deputy Lodge Manager have day-to-day responsibility for the monitoring of the CCTV System and the implementation of this policy. They are responsible for maintaining a full record of incidents using the appropriate forms and ensuring that all relevant personnel are informed in a timely manner.

5. System Description

5.1 Any changes to the system will be in compliance with data protection legislation. Privacy Impact Assessments will be carried out prior to any new systems being implemented.

5.2 The areas covered by the College's CCTV system are the buildings and grounds within the Parks Road site curtilage and on the HB Allen Site and the immediate exteriors of such buildings and grounds.

5.3 Notices are positioned at the entrance of both sites. These signs indicate that CCTV monitoring and recording are in use with a contact number for further information.

5.4 The central system:

5.4.1 has a number of IP cameras covering its premises 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

5.4.2 The system comprises: Fixed position cameras and one pan and tilt camera; monitors; multiplexers; digital recorders; information signs

5.4.3 The system operates and records 24 hours a day every day of the year

5.5 The library system consists of one fixed position camera, one digital recorder, and two monitors. This system only records when the library security gates are activated.

5.6 Unmanned aerial devices ('drones') may be used for the purposes of conducting surveys of the buildings and grounds. They will be operated by contractors who hold any relevant licences.

5.7 None of the cameras within the system are installed in a covert manner. Some cameras may be enclosed within 'All weather domes' for operational reasons. None of the areas covered would be considered private.

5.8 The system is not capable of audio recording.

5.9 CCTV images are retained for 30 days, and are then overwritten unless required as part of an ongoing investigation, in which case recordings will be retained for as long as required for that investigation. For internal investigations, recordings will be retained for 6 years after the conclusion of the investigation, in line with the College's retention schedules and ROPAs.

6. Control of Viewing and Access to Live CCTV Data

6.1 Display equipment used to view the images from CCTV cameras will be located and positioned in such a way as only those responsible for security may ordinarily see the screen.

6.2 Where display equipment is provided for controlled access security at a particular place such as a door entry point, display equipment will be located and positioned in such a way that only those likely to operate the system can view the image.

6.3 All viewing and observing of the live CCTV images from the central cameras (see System Description above) will be carried out by authorised users including lodge staff. No unauthorised access to the CCTV screens or recordings will be permitted at any time. Access to the live images will be strictly limited to the lodge staff (including night porters, supplied by Oxford Security Services), the DPO, the Domestic Bursar, the Head of Rooms Division, the HR

Manager, the IT Manager and Senior IT Officer. The College IT staff may be asked to access pre-recorded images, in order to facilitate duplication etc.

6.4 In addition to the central CCTV system, the Library operates cameras, primarily to prevent and investigate book theft. Library staff are able to view images from these cameras from within the Library. The operation of the camera and the viewing of images by Library staff must be managed in line with this policy.

7. Access to/Disclosure of Pre-Recorded CCTV Data

7.1 For the central system, full system access will be strictly limited to HR Manager, IT Manager, Senior IT Officer, Rooms Division Manager, Lodge Manager, Deputy Lodge Manager and the DPO. The College IT staff may be asked to access pre-recorded images, in order to facilitate duplication etc.

7.2 For the library system, the viewing of recorded images is based on the recording being triggered by the security system. Access to pre-recorded images is limited to the library staff. The time stamp of the recording may be combined with card access data to investigate any incidents.

7.3 Viewing of the recorded images should take place in a restricted area. Other employees, students and members of the public should not be allowed to have access to that area when a viewing is taking place.

7.4 Requests for access to, or disclosure of images recorded by the CCTV systems from a third party will only be granted if the requestor falls within the following categories:

7.4.1 Data Subjects (persons whose images have been recorded by the CCTV system)

7.4.2 Law enforcement agencies

7.4.3 An authorised College member who has responsibility for welfare

7.4.4 An authorised College member who has responsibility for student discipline – in the course of a student disciplinary investigation

7.4.5 An authorised College member of staff in the investigation of a Health and Safety at Work Act incident

7.4.6 An authorised College member of staff in the investigation of crime

7.4.7 Relevant legal representatives of A Data Subject

7.5 Employees should be aware that CCTV footage may be used and relied upon, where necessary, for discipline purposes. Similarly, if there were allegations of criminal activity by employees or claims brought against any member of the College leading to civil proceedings by students or employees, the College may use and/or submit the relevant footage to the relevant authorities.

7.6 Internal requests are most likely to come from the Bursar, Domestic Bursar, Dean, HR Manager, Welfare Fellow, Student Support Officer, Rooms Division Manager or Lodge Guest Relations Manager. Requests from anybody else will be less likely to be authorised. Requests will be processed by those staff listed in 7.1 above as having full access. They may only share CCTV data following authorisation by the Bursar, the Domestic Bursar or the DPO. The person sharing the data must have received permission directly from the authoriser, not anecdotally from the requester. Nobody may authorise their own access to or processing of CCTV data. External requests will require authorisation from the Bursar, Domestic Bursar or DPO. If the request is received from the data subject or somebody acting on their behalf, this must be referred to the DPO and handled as a Subject Access Request.

7.7 The College will keep a record of the date of disclosure of personal information relating to identifiable individuals, which has been captured through CCTV, along with details of who the information has been provided to,

why they required it and their lawful basis for processing the data. This will be recorded by the person who authorised the disclosure of the CCTV data. The person receiving the data will be reminded that it may only be used for the purpose access was authorised and may not be shared with third parties without consulting the DPO.

7.8 Where we receive a valid request for images, they must be shared in a secure manner. Further details on this can be found in the CCTV Operations Manual. These images are retained for two months on a secure password protected server, in case there are any further requests, or if there has been a technical issue. After two months these images are deleted by the Domestic Bursar.

8. Access to Images by a Law Enforcement Agency

8.1 Law enforcement agencies may view or request copies of CCTV images subject to providing an appropriate written request, and in accordance with the protocols contained in this document. A warrant number and crime reference should be given, with identification checked. Normal procedures for authorisation will be followed and images will be shared after authorisation has been received, unless it is in relation to an emergency (see 9.1-2).

9. Access to Images in an Emergency

9.1 In situations where there is a genuine risk of physical harm (such that the lawful basis of 'vital interests' might apply) or where the lawful basis of 'legal obligation' might apply, immediate access to images may be given to the Welfare Fellow, Dean, Junior Deans, Student Support Officer or emergency services. The access must be necessary and proportionate.

9.2 The Operations Manual will include procedures that those receiving the request should follow, in terms of seeking authorisation and access outside of office hours.

10. Access to Images by a Data Subject or a Member of the Public

10.1 CCTV digital images, if they show a recognisable person, are Personal Data and are covered by data protection legislation. 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 legislation (see 10.5). They do not have a right to instant access.

10.2 A person whose image has been recorded and retained and wishes to have access to the data should apply via the Subject Access Request Form. The request must state the date, time and location that the footage was captured, any other useful information i.e. hair colour, clothing, direction of travel and number of people will help speed up the search.

10.3 All Subject Access Requests (SAR) must be made by the subject themselves, or their legal representative, and handled by the DPO.

10.4 Additionally persons may make a Freedom of Information Act (FOI) request.

10.5 FOI and SAR requests will be processed promptly. In the case of a Freedom of Information Act requests a response will be sent within 20 days. In the case of a Subject Access Requests, made under UK GDPR, a copy will be provided within one month. All requests will be formally acknowledged; however, in both cases, the legislation allows certain exemptions, for example preventing the sharing of third party personal data, so requested information may be withheld.

11. System Maintenance

11.1 Display equipment and recordings may be viewed by personnel authorised to undertake installation and maintenance of the CCTV systems. Such viewing will be restricted to that necessary for system work.

11.2 Contractors working on the system will sign an undertaking that they understand and will comply with Keble College, CCTV Policy Standards and Procedures.

12. Policy Review

12.1 This policy may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

12.2 This policy was approved by DPISC on 21 January 2026. It should be reviewed in January 2027.