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 (currently the General Data Protection Regulation ("GDPR") and the Data protection Act 2018 ("DPA 2018")) and in accordance with legal requirements including the CCTV Code of Practice issued by the Information Commissioners Office and Article 8 of the Human Rights Act 1998 – Respect for Private and Family Life.

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

1.3 For the purposes of the Data Protection Act, 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 Article 5 of the GDPR.

3. Objectives

The objectives of the CCTV system which form the lawful basis for the processing of data 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 Bursar is the College's Data Protection Officer and 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. He can be contacted via email at data.protection@keble.ox.ac.uk.

4.2 The Domestic Bursar is the overall manager for this system, has overall responsibility for ensuring the implementation of this policy, and for handling requests for access to/disclosure requests for CCTV. 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 Head Porter has day-to-day responsibility for the monitoring of the CCTV System and the implementation of this policy. The Head Porter is 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.

5.2 The areas covered by the College's CCTV system are the buildings and grounds within the main 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 in Parks Road

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 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.

5.7 The system is not capable of audio recording.

5.8 CCTV images are retained for 31 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 Data Protection retention policy.

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 the lodge. 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 duty porters (including night porters, supplied by Oxford Security Services), the Data Protection Officer, the Domestic Bursar.

6.4 In addition to the central CCTV system, the Library operates a single camera, primarily to prevent and investigate book theft. Only Library staff are able to view images from this single camera 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, access to pre-recorded images will be strictly limited to the Data Protection Officer, Domestic Bursar, Dean or Head Porter. 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 student discipline – in the course of a student disciplinary investigation

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

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

7.4.6 Relevant legal representatives of A Data Subject

7.4.7 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

7.5 Such access may only be granted by the Data Protection Officer or the Domestic Bursar.

7.6 The College will keep a record of the date of disclosure along with details of who the information has been provided to and why they required it.

7.7 Where we receive a valid request for images, they are normally copied to a USB stick, 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. 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.

9. Access to Images by a Subject

9.1 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 a right to instant access.

9.2 Additionally persons may make a Freedom of Information Act request.

9.3 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.

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

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

9.6 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 form is refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

9.7 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.

10. System Maintenance

10.1 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.

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

11. Policy Review

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

11.2 This policy was approved by DPISC in October 2019. It should be reviewed in October 2020.