Access Control Policy

1. Purpose

1.1 This policy seeks to ensure that the Access Control 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 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 Access Control 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 Access Control 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 Access Control system will be processed in accordance with Article 5 of the GDPR.

3. Objectives

The objectives of the Access Control 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

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 Access Control. 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 Access Control system.

4.4 The Lodge Guest Relations Manager and H B Allen Centre Manager have day-to-day responsibility for the monitoring of the Access Control 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 Access Control 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 Information about the College's Access Control system can be found in the College Handbook, privacy notices and ROPAs.

5.4 The system:

5.4.1 has a number of locks using Salto card or fob access being transmitted to a secure server for storage and for recall at a later date

5.4.2 The system comprises: Salto software, computers and access points for doors and zones

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

5.5 Access Control data is retained for 6 months. 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. Access to/Disclosure of Access Control Data

6.1 Access to Access Control data will be strictly limited to the Data Protection Officer, Domestic Bursar, Lodge Guest Relations Manager, and H B Allen Centre Manager. The College IT staff may be asked to access the data, in order to facilitate duplication etc.

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

6.2.1 Data Subjects (persons whose movements have been recorded by the Access Control system)

6.2.2 Law enforcement agencies

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

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

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

6.2.6 Relevant legal representatives of A Data Subject

6.2.7 Employees should be aware that Access Control data 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 data to the relevant authorities

6.3 Internal requests are processed by the Lodge Guest Relations Manager and H B Allen Centre Manager, under the direction of the Domestic Bursar. External requests are processed by the Data Protection Officer.

6.4 The College will keep a record of the date of disclosure of personal information relating to identifiable individuals, which has been captured through Access Control, along with details of who the information has been provided to and why they required it.

6.5 In the process of responding to a valid request for Access Control data, a report may initially be downloaded and saved to a secure drive within the College system. This data is 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 Access Control data 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 Access Control records are Personal Data and are covered by the Data Protection Act. Anyone who believes that their access has been recorded by the Access Control system 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.

9.3 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 access was captured, any other useful information which will help speed up the search. In the case of a Subject Access Request a copy will be provided within one calendar month.

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

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.

9.2 Additionally persons may make a Freedom of Information Act request. Freedom of Information Act requests must be responded to within 20 days.

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 Access Control data. 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 Access Control data may be viewed by personnel authorised to undertake installation and maintenance of the Access Control 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, Access Control 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 April 2021. It should be reviewed in April 2022.