CCTV Policy

Policy no:	8.2
Version no. & date:	23.3
Next review due:	September 2024
Responsible Committee:	SMT
Approved by & date:	May 2023
Linked policies:	Data Protection Policy Policy on Rights in Relations to Individual's Data
External references	Data Protection Act 2018

	General Data Protection Law
	UK Quality Code UKSCQA/02 Advice and Guidance on Monitoring and Evaluation (6.7) *Providers take account of ethics and data protection requirements when designing and operating monitoring and evaluation systems.*
	ICO No. Z1097339
	Bulletproof (Bulletproof.co.uk) for GDPR Consultancy and Support
Audience:	External

Contents

1 Introduction

Oxford Business College (referred to as “the College”,“we”, “us”, “our”) uses closed circuit television

(CCTV) cameras to provide a safe and secure environment for staff, students, suppliers and visitors and to protect the College property.

The purpose of this Policy is to regulate the management, operation and use of the CCTV system at the College. This document sets out the purpose, accepted use and management of the CCTV equipment and images to ensure that we comply with relevant data protection and privacy laws including: the General Data Protection Regulation and the Data Protection Act 2018 (together referred to as the “GDPR”), and; related laws including but not limited to, the Human Rights Act 1998 (“CCTV Laws”)

This policy has been produced in line with the Information Commissioner’s Office (“ICO”) CCTV Guidance. We may amend this policy at any time. CCTV images are monitored and recorded in strict accordance with this policy.

Images recorded by surveillance systems are Personal Data which must be processed in accordance with data protection laws. The College is committed to complying with its legal obligations and ensuring that the legal rights of staff, relating to their Personal Data, are recognised and respected.

2 Purpose of CCTV

We have considered and determined that the purposes for which the CCTV is deployed are legitimate as well as being reasonable, appropriate and proportionate. We have installed CCTV systems to:

- to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;
- for the personal safety of staff, students, visitors and other members of the public 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 disciplinary or grievance proceedings against staff and students; and
- to monitor the security of campus buildings

3 Our Lawful Basis

Where our use of CCTV involves the processing of personal data for the above purposes, we will rely on the following lawful bases:

- processing is necessary for compliance with a legal obligation (for example, where processing relates to health & safety obligations or where we are obligated to provide information to law enforcement); and

- processing is necessary for the purposes of the legitimate interests of us or a third party, but only where these interests are not overridden by the rights and freedoms of the data subject (for example, processing relating to security purposes and our general use of CCTV).

We may also process personal data relating to our use of CCTV where it is necessary for the establishment, exercise or defence of legal claims. We will not carry out automated decision making or profiling in respect of our use of CCTV.

4 Operation Overview and Responsible Staff

The CCTV system is owned by the Oxford Business College and managed by the College and its appointed users on local campuses.

The Head of Operations is responsible for the overall management and operation of the CCTV systems across the College, including it's installations. The Head of Operations and delegated staff for all local campuses are responsible for the management and operation of their local CCTV systems including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.

Cameras will be used to monitor activities within the College buildings and other areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the occupants within the College grounds, together with its visitors. The CCTV system operates across the various campuses of the College in different locations. See **Annex-1** for the locations of CCTV.

Signs are placed at all pedestrian and vehicular entrances in order to inform staff, students, visitors and members of the public that CCTV is in operation. The signage indicates that the system is managed by the College and contact information is provided.

5 Monitoring and Recording

All our maintained cameras are readily visible to any person in the vicinity with suitable signage displayed. As their usage is to monitor the general activities happening in the vicinity, such monitoring is not covert and authorisation is not required.

CCTV cameras located in the College record are monitoring 24 hours a day and this data is continuously recorded. Authorised CCTV users on local campuses will receive training and access to written procedures for maintaining and respecting the privacy of visitors, staff, suppliers, students and other individuals who might appear in the footage.

Images are recorded locally and are on hardware that is securely kept on local campuses and are only viewable by authorised staff.

6 Retention

Images and recording logs must be retained and disposed of in accordance with our Data Retention Policy for IT Facilities.

CCTV images held on the hard drive of a PC or server will be overwritten on a recycling basis once the drive is full, and in any event, will not be held for more than 30 days, without prior authorisation by the Operations Manager for reasons which are recorded and notified to the Head of Compliance.

Access to retained CCTV images is restricted to the Head of Operations and other persons as required and as authorised by the Head of Operations or the Managing Director.

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.

7 Third Party Access to Images

Access to and disclosure of images recorded on CCTV will be restricted and carefully controlled. This will ensure that the rights of individuals are protected, and also ensure that the images can be used as evidence if required. Images may only be disclosed in accordance with the purposes for which they were originally collected.

Disclosures to third parties will only be made in accordance with the purposes for which the system is used and will be limited to:

- police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and / or the prevention of terrorism and disorder;
- prosecution agencies (such as the Crown Prosecution Service);
- relevant legal representatives of people whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings);
- where the disclosure is required by law or made in connection with legal proceedings;
- in exceptional cases, for others (such as insurers) to assist in identification of a victim, witness or perpetrator in relation to a criminal incident; and staff involved with our disciplinary processes.

A request for images made by a third party should be made in writing to the Head of Operations. Disclosures will be made at the discretion of the Head of Operations, with reference to relevant legislation and where necessary, following advice from the Head of Compliance and the DPO.

If images are sought by third parties, including the police, evidence of statutory authority to request the information will be required before CCTV images are disclosed. Head of Operations will certify that the images are required for an instance such as: (i) an investigation concerning national security, (ii) prevention or detection of crime, or (iii) the apprehension or prosecution of offenders or (iv) it is required by law or made in connection with legal proceedings.

Where possible, viewing of recorded images will always take place in a restricted or secure area to which other members of staff will not have access while viewing is occurring. If images belonging to other data subjects removed/blurred from the recording for viewing purposes, this will be documented and a record will be kept. Images retained for evidence will be securely stored with limited access for authorised staff only.

A record of any disclosure made under this policy will be held on the CCTV management system, itemising the date, time, camera, requestor, authoriser and reason for the disclosure.

8 Data Subject Rights and Access to Images

The GDPR gives individuals the right to access personal data about themselves, including CCTV images and footage. Individuals may exercise this right through what is known as a data subject access request (DSAR). Such requests can come in any format, however in order to locate the images on the College's system, sufficient detail must be provided by the data subject in order to allow the relevant images to be located and the data subject to be identified.

Furthermore, data subjects also have the right to:

- have their personal data corrected where it is inaccurate;
- have their personal data erased where it is no longer required (provided that we do not have any continuing lawful reason to continue processing their personal data);
- have their personal data transferred to another individual/organisation in an appropriate format;
- object to the processing of their personal data
- withdraw their consent to processing (where consent is our lawful basis); and
- restrict the processing of their personal data.

9 Complaints

Complaints concerning the College's use of its CCTV system or the disclosure of CCTV images can be made by emailing complaints@oxfordbusinesscollege.ac.uk

All individuals affected by this Policy have the right to make a complaint to the Information Commissioner's Office at any time.

By Post:

Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

By Website: Click Here https://ico.org.uk/concerns/complaints-and-compliments-about-us/

By Email: Click Here https://ico.org.uk/concerns/complaints-and-compliments-about-us/

By Phone: 0303 123 1113 (Local rate) or 01625 545 745 (National rate)

10 Monitoring Compliance

All staff involved in the operation of the College's CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein. All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake data protection training.

11 Policy Review

This document is reviewed periodically as part of our internal procedures. We take data protection very seriously, and strictly adhere to the rules laid out in data protection laws. This policy was last updated on 26/04/2023

We may update this policy from time to time and circulate a new version internally. Any amendments to this policy will require a Data Protection Impact Assessment be carried out, to evaluate and mitigate risks conferred upon data subjects.

Appendix

Link for CCTV External Agency Form: