Oxford Sixth Form College

A NORD ANGLIA EDUCATION SCHOOL

CCTV Policy

Revised: June 2024

Review date: June 2025

Contents

CCTV AND ELCTRONIC DOOR ACCESS SYSTEMS AND BUILDING SECURITY

INTRODUCTION

Oxford Sixth Form College (OxSFC) values its reputation and is committed to maintaining the highest levels of conduct and integrity to ensure compliance with ethical standards and legal requirements.

The need to maintain a safe environment for the protection of the personal safety of staff and student is of the utmost importance Oxford Sixth Form College.

POLICY STATEMENT

This policy seeks to ensure that the Closed-Circuit Television (CCTV) system and door access control system used on OXSFC premises is operated in compliance with the law relating to data protection. It takes into account best practice as set out in codes of practice issued by the Information Commissioner (ICO).

OXSFC seeks to provide safe and welcoming environment to its students and to ensure, as far as reasonably practicable, the safety and security everyone on its properties (OXSFC Sites). OXSFC therefore, deploys CCTV and door access controls to:

1. Promote a safe environment and to monitor the safety and security of OXSFC Sites.
2. Ensure public, staff, parents or guardians, students and employees safety.
3. Deter crime.
4. Assist in the prevention, investigation and detection of crime and other misconduct.
5. Reduce the fear of crime and to reassure staff, parents or guardians, students and employees.
6. Assist in the identification, apprehension and prosecution of offenders.
7. Assist in the investigation of accidents.

OXSFC's door access control system is an electronic system whereby certain doors are permanently held in the closed or locked position and access, or egress can only be gained via the use of a preprogrammed Identification (ID) card.

This policy will be reviewed annually by the Data Protection Officer (DPO) to ensure the use of CCTV and door access systems for the above purposes remains justified and any changes are approved by the Principal.

This policy does not form part of employees' terms and conditions of employment and may be subject to change at the discretion of OXSFC's management.

SCOPE

For the purposes of this policy, this policy applies to the use of CCTV and door access systems and includes systems:

- Deployed in public areas;
- For recording or viewing visual images for security purposes;
- For recording user's door access for security purposes; and
- For storing, receiving, transmitting, processing or checking images or information obtained by the systems above.

This policy is limited to systems where OXSFC is data controller.

Annex 1 contains protocols for notifying students of systems where OXSFC is not data controller, e.g. in certain boarding accommodation where OXSFC's landlord is deemed data controller.

GENERAL RULES FOR MAINTAINING BUILDING SECURITY

Maintaining the physical security of offices and rooms where information, data and processing facilities are accessed and located is vitally important. There must be methods of physically securing access to protect information, data and personal belongings:

1. Staff and students must wear their ID badges and visitors must wear the Visitor ID badges which have been issued to them.

2. People who are not displaying ID badges should be challenged if it is safe to do so. Any person not known to location personnel must be challenged to establish who they are and whether authorisation has been provided for them to be there. If there is any doubt about the identity of the individual or there is a general safety concern about challenging them, an SMT manager should be contacted to confirm the individual's identity and consider appropriate action to take.

3. A visitor log needs to be in place to record the names, dates, times and signatures for the signing in and out of to college locations. All visitors must be issued with an visitors' badge when signing in to OXSFC controlled premises by the reception team. All visitors should be met by a relevant staff member.

4. The use of keys to buildings, rooms, secure cabinets, safes etc. must be controlled and recorded by the Estates and Facilities team. Keys must be stored in secure areas/locked cabinets when not in use and must be identifiable by recording serial/ID markings of all keys. The location of keys must be known at all times and a signing in/out recording mechanism must be maintained to record the serial/ID of keys against individual names when keys are used.

5. Electronic access cards must be issued to authorised staff and students by the IT department on an individual basis. Staff and student issued with access cards must have their names and pictures on them.

6. Access cards should only be used by the registered user and must not be lent out or given to other staff or students, regardless of their seniority.

7. Access cards issued to personnel who no longer work or study at the college must be deactivated and recovered immediately by the IT team.

8. Access to and knowledge of cards, door lock codes or access to keys for locks, are restricted to authorised personnel only such as IT and Facilities teams and must not be shared with any unauthorised person.

CCTV SYSTEM CAPABILITIES

The capabilities of security camera systems are subject to development and change in line with technological developments. Systems must always be capable of performing the function for which they are deployed.

PROVISIONS FOR THE USE OF CCTV SYSTEM

CCTV systems seek to strike a balance between meeting the need for security and avoiding the possibility of intruding into individuals' privacy.

The deployment, management and operation of security cameras across the business adhere to the provisions set out within this policy. These maintain a balance between public protection and individual privacy, establish the rationale for the systems, ensure compliance with other legal duties and, by building public confidence, assist in achieving surveillance by consent.

RESPECT FOR PRIVACY

Security camera and door access systems are only used in areas where there is considered to be a particularly high risk of intrusion or vulnerability or that can reasonably be regarded as public places / high traffic area. CCTV will not be used where there is a high expectation of privacy (e.g. bedrooms/toilets/classrooms).
They are not used to actively monitor staff and students' whereabouts. In addition:

• Areas under CCTV coverage are routinely reviewed to ensure the capability meets the purposes set out.

• Security camera systems do not record conversations.

However, the college does reserve the right to check staff and student locations as part of an investigation or complaint.

CCTV systems installed by OXSFC are standard CCTV systems and do not use facial or other biometric characteristic recognition technology. Any use of facial or other biometric characteristic recognition technology must have a Data Privacy Impact Assessment carried out as these are privacy intrusive technologies which is reviewed by the Data Protection Officer and NAE's Central Compliance Team prior to approval by the Principal.

New systems or if when CCTV monitoring is extended into new areas OXSFC must conduct a Data Privacy Impact Assessment to ensure that the purpose of the system is justifiable and not privacy intrusive. OXSFC recognises that these are privacy intrusive technologies which is reviewed by the Data Protection Officer and NAE's Central Compliance Team prior to approval by the Principal.

The DPO will maintain a CCTV and Door Access Log Register to log all system access requests from OXSFC staff. All data subject rights requests will be logged in the standard form.

TRANSPARENCY OF USE OF CCTV

OXSFC will ensure that there are clearly displayed signs to inform people that CCTV is in operation with the reason for its use and that they should contact the DPO with any queries. Notices for CCTV must be displayed clearly visible, legible and placed so that the data subjects are aware that they are entering an area which is covered by video surveillance. Notices must be made age appropriate particularly for where CCTV captures images of students.

VIEWING OF CCTV IMAGES AND DOOR ACCESS LOGS BY OXSFC TEAM MEMBERS

The following OXSFC Team Members have the authority to view saved images without prior approval, but access must be recorded by the DPO:

- NAE Europe Regional Managing Director and OXSFC Principal for any serious incidents or safeguarding concerns
- OXSFC or NAE Health & Safety Manager for H&S incidents or accident reporting purpose
- HR team members responsible for disciplinary and complaints investigations and related proceedings

All other OXSFC Team Members require permission from the Principal and DPO.

Live CCTV must be viewed only on approval of the DPO or Principal in exceptional circumstance. Exception to this is for the staff responsible for maintaining security at St Ebbes and Pensons Gardens where live CCTV is used to actively monitor the entrance and manage access to the building.

Should it become apparent, in the course of an investigation, that a criminal offence may have been committed, then the Principal or the Regional Managing Director must be informed immediately.

Any safeguarding concerns identified in CCTV footage must be notified to the Designated Safeguarding Lead and Principal immediately.

CCTV evidence may be used as part of an employee investigation where, in the reasonable belief of OXSFC, it will assist in the effective resolution of disputes which arise in the course of disciplinary and grievance proceedings. It may also be used to assist in the defence of any civil litigation including employment tribunal proceedings. In such cases the footage must be requested by the HR Manager. In accordance with the ICO CCTV Code of Practice, where footage is used in disciplinary proceedings, the footage will be retained, and the worker allowed to see and respond to the images. In the case of a contractor or non-OXSFC employee any evidence identified may be passed to a third party, such as the individual's employer.

COMPLAINTS

OXSFC aims to manage issues and concerns around CCTV and door access systems as quickly as possible.

Any complaint must be immediately passed to the Data Protection Officer for formal response and record keeping. The Data Protection Officer will acknowledge receipt of the complaint promptly and then provide a written response will be sent to the complainant within 30 days.

OXSFC will also provide an escalation the complaint to the NAE Group Data Protection Officer (compliance@nordanglia.com) for review and further consideration to the complainant.

STORAGE OF IMAGES AND INFORMATION

CCTV recordings will always be maintained and footage continuously recorded and held on system memory for a period of 30 days.

Door access logs are retained for a full academic year and purged annually during the summer holidays.

If there is a legitimate reason for retaining the CCTV images or door access logs for longer (such as for use in an accident investigation, disciplinary investigation and/or legal proceedings), then the data may be retained for a limited extension. For CCTV, the footage or still frames can be isolated and saved out of the CCTV system in an appropriately secure system. For door access logs, relevant data can be

extracted into a text file. All retained data must be stored securely (e.g. password protected folder with limited access managed by the Data Protection Officer; encrypted physical hard drive stored securely). Any recordings kept for legal proceedings must follow protocols set by the Central Legal Team (e.g. specific evidential requirements for securing evidence for proceedings.

Any retained data on an OXSFC device or SharePoint folder must be deleted or destroyed once they are no longer needed for the purpose for which they were saved. The Data Protection Officer will review monthly any footage retained beyond the 30-day period to ensure that the justification to retain is valid.

DATA SUBJECTS RIGHTS

Recorded CCTV images and door access logs are considered to be the personal data where individual are identifiable.

Data subjects have a right to access to their personal data. They also have other rights, in certain circumstances, including the right to have their data erased, rectified, and to restrict processing and object to processing.

On receipt of any rights request, the request must be provided to the Data Protection Officer immediately. The Data Protection Officer will manage the rights request in line with the OXSFC Data Subject Rights protocols.

The full response to any data subject rights request must be provided without undue delay and at the latest within one month of receiving the request unless the request is extensive, and an extension of the period is justified. OXSFC acknowledges that a request requiring CCTV footage is not sole grounds for an extension.

The Data Protection Officer will keep a log of all subject rights requests.

The DPO must also consider if any exemptions apply to the request. This may include to protect the rights of other data subjects. If the footage requested contains images of other people, the DPO must consider the most appropriate means of disclosure which may include:

- use of technology to deidentify other data subjects; or
- obtaining consent from the other data subjects to disclose their personal data.

The DPO will keep a record of all disclosures which sets out:

- when the request was made and by whom and the response times
- Any exemption applied (including protection of the rights of other individuals)
- Format of the disclosure

OXSFC recognises that it may only refuse a data subject access request if the request is:

- manifestly unfounded; or
- manifestly excessive.

The IT team will provide the DPO with a secure means of delivering data subjects copies of their data, such a secured SharePoint portal with limited access. OXSFC may retain copies of subject access requests for a period of 12 months.

THIRD-PARTY ACCESS

Third party requests for access will only be considered, in line with the data protection legislation. The DPO will keep a record of all third-party requests and their outcomes.

Legal representatives of Data Subjects:
Where legal representatives of Data Subject makes a data subject rights request (including access to data on the systems), the recipient of this must immediately forward it to the DPO. The legal representatives will be required to submit to the DPO a letter of authority to act on behalf of the data subject together with the evidence of the Data Subject's identity.

The DPO will manage the request in line with the data subject rights requests set out above.

Disclosures required by law or in connection with legal proceedings:
Where requests for disclosures are required by law or in connection with legal proceedings, such requests must be sent to the Principal and the DPO. They will review the request in line with data privacy and other legal obligations.

Requests from the Police or law enforcement:
The recipient of this request should forward it to the DPO. They will review the request in line with data privacy and other legal obligations.

OXSFC will only consider these requests if it is made formally under Schedule 2 Part 1Paragraph 2 of the Data Protection Act 2018. The form should provide information about the requesting officer, the reason for the request and details about the information requested (i.e. from which camera, on which date, time, etc).

The DPO is only authorised to make disclosures to law enforcement agencies on grounds of:
1. an investigation concerning national security; or
2. the prevention or detection of crime; or
3. the apprehension or prosecution of offenders, and that the investigation would be prejudiced by failure to disclose the information.

The DPO will consult with the Principal prior to making any disclosure to law enforcement.

The IT team will provide the DPO a secure means of delivering copies of the data requested to any third party and the DPO will assess the retention period for each third-party disclosure and ensure that this is maintained.

CONSEQUENCE OF NON-COMPLIANCE WITH THIS POLICY

Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal.

ANNEX 1- PROTOCOLS FOR CCTV SYSTEMS WHERE OXSFC IS NOT DATA CONTROLLER

For Premises Controlled by IQ Students at Alice House

NOTICE TO OXSFC STUDENTS and STAFF

The CCTV on this premise is managed by: IQSA (Oxford) Limited t/a IQ Students, registered address: 7th Floor Cottons Centre, Cottons Lane, London, United Kingdom, SE1 2QG and they are data controller for the personal data collected on the premises. Their privacy notice can be found here: https://www.iqstudentaccommodation.com/privacy-centre

Recorded images of individuals captured by CCTV cameras are considered personal data of those individuals.

This means any images recorded of you on CCTV in this accommodation is your personal data and you have a right to exercise your personal data rights regarding this data. This includes the right to access – e.g. obtain a copy of that data.

You can request a copy of the CCTV or any other data from the data controller (named above) who controls this accommodation by emailed their Data Protection Officer ('DPO') at

DPO@iqstudent.com

We recommend you are specific in the date(s), time(s), and locations for which you want to have the video or other personal data.

They should acknowledge your request in 2 days and respond within a month of the request. They cannot charge a fee except in rare circumstances.

They can ask for copies of identification documents from you including a current picture to help them identify you in the CCTV.

You will not be entitled to images of other people unless they have given permission.

If you need help in exercising your rights, please contact your house parent or by using the online form on the Information Commissioner's Office (ICO) website: https://ico.org.uk/for-the-public/getting-copies-of-your-information-subject-access-request/

If you are not satisfied with how your request has been handled, then you can complain to the data controller by contacting their DPO by email: DPO@iqstudent.com

OR

Contacting the ICO which regulates data privacy in the United Kingdom by completing their online form: https://ico.org.uk/make-a-complaint/data-protection-complaints/personal-information-complaint/

For Premises Controlled by Capital Students at properties such as Student Castle

NOTICE TO OXSFC STUDENTS and STAFF

The CCTV and door security systems on this premise is managed by: S.C. Osney Lane Management Limited (t/a Student Castle), registered address: Kintyre House, 70 High Street, Fareham, Hampshire, England, PO16 7BB and they are data controller for the personal data collected on the premises. Their privacy notice can be found here: https://www.studentcastle.co.uk/privacypolicy/

Recorded images of individuals captured by CCTV cameras and the security logs connected to their door passes are considered personal data of those individuals.

This means any images recorded of you on CCTV in this accommodation and data recorded about your door pass are your personal data and you have a right to exercise your personal data rights regarding this data. This includes the right to access – e.g. obtain a copy of that data.

You can request a copy of your personal data from the data controller (named above) who controls this accommodation by emailed their Data Protection Officer ('DPO') at

dpo@studentcastle.co.uk

We recommend you are specific in the date(s), time(s), and locations for which you want to have the video or other personal data.

They should acknowledge your request in 2 days and respond within a month of the request. They cannot charge a fee except in rare circumstances.

They can ask for copies of identification documents from you including a current picture to help them identify you in the CCTV.

You will not be entitled to images of other people unless they have given permission.

If you need help in exercising your rights, please contact your house parent or by using the online form on the Information Commissioner's Office (ICO) website: https://ico.org.uk/for-the-public/getting-copies-of-your-information-subject-access-request/

If you are not satisfied with how your request has been handled then you can complain to the data controller by contacting their DPO by email: dpo@studentcastle.co.uk

OR

Contacting the ICO which regulates data privacy in the United Kingdom by completing their online form: https://ico.org.uk/make-a-complaint/data-protection-complaints/personal-information-complaint/