Wolfson College
Cambridge

CCTV Policy and Code of Practice

Introduction

Wolfson College uses a closed-circuit television (CCTV) surveillance system on its premises as part of our efforts to provide a safer and secure environment for our members and visitors. This Policy sets out the appropriate actions which must be followed to comply with the following legislation in respect of the use of CCTV surveillance system:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Biometrics and Surveillance Camera Commissioner's Surveillance Camera Code of Practice
- Human Rights Act 1998.

Ownership and Copyright

The CCTV system, all recorded material and copyright is owned by Wolfson College, Barton Road, Cambridge CB3 9BB.

Purpose

The system is installed to:

- Detect, prevent or reduce the incidence of crime, public disorder and damage to property.
- Reduce the fear of crime and create a safer community.
- Assist with the apprehension, investigation and prosecution of offenders.
- Improve communications and the operational response of security patrols.
- Assist in managing health and safety issues by detecting potential incidents.

This policy intends to:

- Inform all who come onto the College site that CCTV is in use.
- Keep CCTV data secure and controlled by authorised staff members.
- Ensure CCTV data is used for stated purposes only.
- Prevent unauthorised access to CCTV images.

Any changes to the purposes for which the CCTV system is used will require prior approval of the College Data Protection Lead and College Council.

Scope

This policy applies to members of staff, fellows and students, visitors to the College and all other persons whose images may be captured by the CCTV system.

Data Protection

CCTV images of identifiable living people fall within the scope of the Data Protection Act 2018. The College is registered with the Information Commissioner's Office (registration number Z9657593) and is the Data Controller for the images produced by the system.

The College has carried out a Data Protection Impact Assessment (DPIA) and based on the findings, considers it necessary and proportionate to install and operate a CCTV surveillance system. The purpose(s) for siting each camera is recorded in the Data Protection Impact Assessment. All processing of personal data will be handled in accordance with the 12 guiding principles of the **Biometrics and Surveillance Camera Commissioner's Surveillance Camera Code of Practice**.

Data Breaches

Unauthorised access to, or disclosure of CCTV images will constitute a breach of data protection legislation and should be reported immediately to the College Data Protection Lead. (The College is legally required to report data breaches to the Information Commissioner's Office (ICO) within 72 hours.)

Tampering with cameras, monitoring or recording equipment, and unauthorised access, copying, disclosure or possession of CCTV images will be regarded as a serious disciplinary matter, investigated and dealt with according to the College's disciplinary procedure; a process which could ultimately result in the dismissal of any member of staff who is responsible for the breach.

About the CCTV system

The system comprises several cameras with no physical zoom or tilt functionality. Some of the cameras have a fisheye lens that digitally simulates tilt and zoom. Most cameras have the capability for audio recording, but this functionality is disabled. The cameras are linked back to system which is located on a networked device located in Server Room 1 in the Jack King Building. The cameras provide good quality images which are adequate for the detection and investigation of crime and are constructed to be as vandal-proof as possible.

CCTV cameras are installed at perimeter gates, building entrances, car parks, inside buildings and public areas which are considered to be vulnerable and operate 24-hours a day, throughout the year. All cameras are sited in prominent positions where they are clearly visible, to meet the purposes for which the CCTV is operated. Cameras will not be sited, so far as possible, to record areas that are not intended to be the subject of surveillance. The College will make all reasonable efforts to ensure that areas outside of the premises and grounds are not recorded.

Where a camera potentially covers private spaces within the College, relevant parts of CCTV images are obscured to ensure privacy is maintained. CCTV cameras will not be used to infringe an individual's right to privacy; areas such as toilets and sleeping accommodation will not be monitored.

The College may occasionally utilise non-functioning, or "dummy" cameras, to increase the deterrence value of the College's CCTV system if there is specific need. All decisions to use non-functioning cameras must be authorised by the Bursar.

Independently installed and operated CCTV systems are not permitted on College property and if found, action will be taken to close such systems down.

System changes

Decisions relating to the installation of new cameras, or the repositioning, or removal of existing cameras, e.g. to fill in a gap in coverage, or respond to building changes, will be made by the Head Porter and Domestic Bursar and approved by the Bursar. The Data Protection Impact Assessment (DPIA) will be reviewed to inform decisions, ensuring privacy implications are carefully considered. The College Data Protection Lead will ensure that the installation remains compliant with the Biometrics and Surveillance Camera Commissioner's Surveillance Camera Code of Practice and the College CCTV Policy.

Signage

Signs are placed at main entrances and other key locations to indicate:

- The presence of monitoring and recording.
- That images are being monitored and recorded for the purposes of crime prevention and public safety.
- Ownership of the system.
- Contact details for the Porters' Lodge.

This will ensure that both the maximum deterrent value is achieved and that College members, staff and visitors are aware they are in an area monitored by CCTV cameras.

Responsibility for the CCTV system

The Bursar has overall responsibility for the implementation and use of the system. The system is managed on a day-to-day basis by the Domestic Bursar, Head Porter and the Business Services & IT Manager. Operation of the system is restricted to the Domestic Bursar, Porters and IT staff. Staff who are authorised to use the CCTV system have the following responsibilities:

- To uphold the arrangements provided in this Policy.
- To handle CCTV data securely and responsibly, within the aims of this Policy.
- To be aware that they could be committing a criminal offence if they misuse personal data captured by CCTV cameras.
- To report any breach of procedure to the College Data Protection Lead.
- To attend training as required.

Staff training

All members of staff who are responsible for operating the CCTV system will be trained in the use of the system relevant to their role and to understand the data protection principles governing its operation.

Directed surveillance

Under normal circumstances, College CCTV will not be used for intrusive or directed surveillance. Decisions on the use of directed surveillance will be made by the Bursar in conjunction with the Domestic Bursar (where staff involvement is suspected), Senior Tutor (for students) or the President (for Fellows). They must satisfy themselves that a sound intelligence case exists, and the use of the directed surveillance is proportional to the incident and likely outcome, while minimising intrusion to

those quite properly going about their normal daily business and whose image may be captured by a directed camera.

Any such covert processing will only be carried out for a limited and reasonable period consistent with the objectives of making the recording and will only relate to the specific suspected unauthorised activity. The decision to adopt covert recording will be documented and will set out how the decision to use covert recording was reached and by whom. Once the purpose for use of a camera has finished, the camera will be disabled or removed.

Access to live footage

Live images captured by the CCTV system are monitored on a real-time basis by Porters in the Porters' Lodge which is a self-contained, secure area. The Lodge must be locked if unstaffed to prevent unauthorised access to CCTV images.

The Head Porter, Porters, Bursar, Senior Tutor and Domestic Bursar may view live feed to obtain information to respond to incidents in College. IT staff access live CCTV images to provide technical support as needed.

Storage, retention and disposal of images

Data captured by the CCTV cameras is stored on a dedicated, secure server located in the College. Images are configured to be automatically overwritten every 31 days unless required as part of an investigation or subject access request. Recordings are made only when motion is detected with five seconds on either side of the detection.

Images retained for internal investigations or criminal proceedings will be accessible only to the Head Porter and those conducting the investigation and will be retained for 3 months following the end of any internal investigation or criminal proceedings.

Requests to view recorded images should be made in writing (using the CCTV Access Request Form) and sent to the College Data Protection Lead who will determine whether disclosure is necessary, legitimate and lawful.

CCTV Register

A CCTV Register will be maintained by the Head Porter. Access to this will normally be restricted to the Head Porter, Bursar and the Domestic Bursar, although the Bursar may authorise access by other members of staff if required.

Viewing recorded images

Access to recorded CCTV images is restricted and carefully controlled to ensure images are only disclosed for the purposes for which they were originally collected. This ensures that the rights of individuals are preserved, and evidence remains intact should images be required for disciplinary or criminal offence investigations.

The Head Porter, Bursar, Senior Tutor and Domestic Bursar are authorised to search CCTV footage stored on the College server to establish if the system has captured images relevant to the incident. Viewing of recorded images must take place in a restricted area to which other employees do not have access.

If the relevant images are held, they will be captured to prevent them from being destroyed. All bookmarked, recorded images will be securely stored until they are no longer needed by the College or are passed to the police or other authorised third party.

All searches of recorded images, together with the reason for viewing, will be noted in the CCTV Register, which is maintained by the Head Porter.

Disclosure of images to third parties

The College will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the purposes for which the system is used and is restricted to external bodies, such as the police and other law enforcement agencies, where the recorded images could assist in the prevention or detection of a crime, the identification and prosecution of an offender, or the identification of a victim or witness. Disclosure to other third parties will only be granted where the needs of the third party outweigh those of the persons whose images are recorded.

The College Data Protection Lead authorises all applications for disclosure of images. Applications to view or release copies of images received from external bodies will only be accepted when a lawful basis for sharing CCTV images has been established. The identity of persons requesting to view CCTV images will be verified. All requests for access to images will be documented in the CCTV Register. The release of CCTV images will be on the basis that at no time can the images be used for anything other than the purpose for which they were originally released.

When CCTV images are released to the police or other authorised persons, they become the Data Processor and are responsible for the security and processing of the data supplied.

On no account should CCTV data be viewed by any unauthorised person, copied or removed from the College without written authorisation from the Bursar.

Subject Access Requests

Individuals who are recorded by CCTV cameras are data subjects for the purposes of data protection legislation and have a right to request access to those images, provided they are recognisable from the image. Any individual wishing to make a Subject Access Request should complete a '**CCTV Subject Access Request Form'** (which can be downloaded from the College website) and send the form to the College Data Protection Lead at: sar@wolfson.cam.ac.uk

Where such a request is authorised, the Head Porter will review the CCTV footage in accordance with the request. Data subjects have no right to access CCTV images relating to other people. If footage contains images of other individuals, the College will consider whether:

- images can be obscured so as not to identify other individuals.
- other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained, and
- it is reasonable in the circumstances to disclose those images to the data subject.

Data subjects will be informed if the College is unable to comply with a request where access could prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

Maintenance

Images produced by the CCTV equipment are intended to be as clear as possible so that they are effective for the purposes specified. The CCTV system is checked daily to ensure that it is operating effectively and showing the correct date and time. Damaged/faulty cameras and system failures should be reported to the IT department. The cameras and system are serviced on an annual basis. Cameras are regularly cleaned, and foliage cut back to maintain clear footage. A maintenance log is kept by the Head Porter.

Compliance

The Head Porter is responsible for compliance with this Policy and the operation of the CCTV system and will conduct an annual review of the use and processing of CCTV images to ensure that the College remains compliant with the laws regulating data protection and privacy. Any complaints or enquiries concerning the operation of the CCTV system should be directed, in the first instance, to the Head Porter: headporter@wolfson.cam.ac.uk

The College Data Protection Lead (the Bursar) has overall responsibility for compliance with data protection legislation. Concerns or enquiries relating to the processing of personal data may be addressed to the College Data Protection Lead at: bursar@wolfson.cam.ac.uk

Review

This Policy is approved by College Council and will be reviewed every 3 years in conjunction with the CCTV Data Protection Impact Assessment (DPIA) to ensure that use of the CCTV system remains justified and compliant with the **Biometrics and Surveillance Camera Commissioner's Surveillance Camera Code of Practice**. A review may also be prompted in response to security incidents or new risks.

Version: 2
Approved by College Council on 18 November 2024
Date of next review: November 2027