
CCTV POLICY

General Council of the Bar



20 February 2020

CCTV Policy

Document type: General Council of the Bar Policy	Date of issue: February 2020 Latest update: May 2022
Author/Originator: Hilary Pook, DPO	Version: V1.02 Review date: May 2023
Status: For internal circulation and website publication	Distribution: All staff
Version history	
V1.01 March 2021	Updated policy to reflect change to UK GDPR Updated checklist at Appendix 2.
V1.02 May 2022	Updated policy to take account of revised guidance from ICO and Biometrics and Surveillance Camera Commissioner. 1.4 Added lawful basis for processing criminal offence data. 5.2 Deleted reference to mobile app as this is not used. 5.3 Changed job title to Facilities Officer. Appendix 1 – removed reference to cameras in the server room as these have been removed, and other minor amendments. Appendix 2 – wording changed to match ICO's new guidance and checks updated.
V1.03 June 2023	Footnote 1: Amended link to ICO guidance 6.3 Added wording in brackets Appendix 1 – set this out on a new form, with minor amendments due to different layout.

1. Policy statement

- 1.1. This policy seeks to ensure that the Closed-Circuit Television (CCTV) system used at the General Council of the Bar (GCB) is operated in compliance with the law relating to data protection, i.e. the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It takes into account best practice as set out in the guidance issued by the Information Commissioner (ICO)¹ and by the Code of Practice issued by the Biometrics and Surveillance Camera Commissioner.²
- 1.2. GCB seeks to ensure, as far as reasonably practicable, the safety and security of all staff and all others that use GCB's offices; and the security of its property and premises. GCB therefore deploys CCTV to:
 - promote a safe office environment and to monitor the safety and security of its premises
 - assist in the prevention, investigation and detection of crime
 - assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings
 - assist in the investigation and breaches of its policies by staff and contractors and, where relevant and appropriate, investigating complaints, and
 - assist in the investigation of accidents.
- 1.3. This policy will be reviewed annually by the Head of Facilities and Property and the Data Protection Officer (DPO) to assure compliance with clauses 1.1 and 1.2 and to determine whether the use of the CCTV remains justified.
- 1.4. The main lawful basis for processing personal data collected via CCTV is Article 6(1)(f) - legitimate interests. GCB has carried out a legitimate interests assessment for operating CCTV in its office. This can be found at [Appendix 1](#). The lawful basis for processing criminal offence data is for the purposes of preventing or detecting unlawful acts (Data Protection Act 2018, Schedule 1 paragraph 10).
- 1.5. There is a check list which is included at [Appendix 2](#).

1 <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/> (undated)

2 www.gov.uk/government/publications/update-to-surveillance-camera-code (2022)

2. Scope

- 2.1. This policy applies to the CCTV systems in the parts of 289-293 High Holborn, London WC1V 7HZ leased by the General Council of the Bar (Bar Council Properties Ltd).
- 2.2. This policy does not apply to other parts of the building, including the exterior and the main entrance area, which are maintained by the landlord.
- 2.3. This policy applies to all GCB staff and contractors.

3. Roles and responsibilities

- 3.1. The Head of Facilities and Property is responsible for ensuring that the CCTV system, including camera specifications for new installations, complies with the law and best practice referred to in 1.1 of this policy. S/he is responsible for the safety and security of the equipment and software utilised for the capture, recording and playback of live and historical CCTV images.
- 3.2. The Head of Facilities and Property is responsible for the evaluation of locations where live and historical CCTV images are available for viewing via the appropriate software. The list of locations and the list of people authorised to view CCTV images is maintained by the Head of Facilities and Property. Diagrams showing the location of CCTV cameras can be found at Appendix 3 [internal version only].
- 3.3. Changes in the use of GCB's CCTV system can be implemented only in consultation with GCB's Data Protection Officer.

4. System description

- 4.1. The GCB operates cameras at the entrances to each of its office floors and in the computer server room on the lower ground floor. They continuously record activities in these areas. (Other cameras operate in other locations in the building which are operated and controlled by the building's landlord.)
- 4.2. CCTV cameras are not installed in areas in which individuals would have an expectation of privacy, such as toilets. Cameras are only located so that they capture images relevant to the purpose the system was set up for. No covert recording is undertaken. No audio is recorded.
- 4.3. CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed near the cameras, so that staff, visitors and contractors are made aware that they are entering an area covered by CCTV. The

signs include contact details of the Data Protection Officer, as well as a statement of purposes for the use of CCTV.

- 4.4. Reception staff must be familiar with the policy and the procedures to be followed in the event an access request is received from either a data subject or a third party.

5. Operating standards

Equipment and access

- 5.1. The images are stored on a Digital Video Recorder (DVR) which is located in the server room.
- 5.2. Images are accessible using the appropriate software and with an authorised user name and password from specific PCs and laptops.
- 5.3. Only the Head of Facilities and Property, the Facilities Manager, and the Facilities Officer have access to the CCTV images.

Processing of recorded images

- 5.4. CCTV images are available only to persons authorised to view them (see above) or to persons who otherwise have a right to view them, such as police officers or any other person with statutory powers of entry. If such visitors are given access to view footage, their identity and authorisation must be checked, and a log retained – see 7 below.
- 5.5. Where authorised persons access or monitor CCTV images on desktops or laptops, they must ensure that images are not visible to unauthorised persons, for example by minimising screens when not in use or when unauthorised persons are present. Screens must always be locked when unattended.

Quality of recorded images

- 5.6. Images produced by the recording equipment must be as clear as possible, so they are effective for the purpose for which they are intended to be used. The standards to be met (in line with the codes of practice referred to in 1.1) are set out below:
 - recording features such as the location of the camera, date and time reference must be accurate and maintained
 - consideration must be given to the physical conditions in which the cameras are located, ie additional lighting or infrared equipment may be needed in poorly lit areas, and

- cameras must be properly maintained and serviced to ensure that clear images are recorded, and a log of all maintenance activities kept.

Retention and disposal

- 5.7. CCTV images are not to be retained for longer than necessary, taking into account the purposes for which they are being processed. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce a 30-day rotation in data retention.
- 5.8. If there is a legitimate reason for retaining the CCTV images (such as for use in an accident investigation, disciplinary investigation and/or legal proceedings), the footage or still frames can be isolated and saved outside the DVR to a separate encrypted zip file. Any saved images or footage will be deleted once they are no longer needed for the purpose for which they were saved.
- 5.9. All retained CCTV images will be stored securely.

6. Data subjects' rights

- 6.1. Recorded images, if sufficiently clear, are considered to be the personal data of the individuals whose images have been recorded by the CCTV system.
- 6.2. Data subjects have a right to access to their personal data under the data protection legislation. 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. They can ask to exercise these rights by emailing the DPO at privacy@BarCouncil.org.uk.
- 6.3. On receipt of a request – which needs to include the date and approximate time of the recording (and a photo of the subject, if appropriate) – the DPO will liaise with the Head of Facilities and Property regarding compliance with the request and communicate the decision to the data subject. This should be done without undue delay and at the latest within one month of receiving the request unless an extension of the period is justified.
- 6.4. If a request is to view footage, and the footage only contains the individual concerned, then the individual may view the footage. The authorised person accessing the footage must ensure that the footage available for viewing is restricted to the footage containing only the individual concerned.
- 6.5. If the footage requested contains images of other people, the DPO must consider:
- whether the images of the other people can be distorted so as not to identify them

- seeking consent from the third parties to their images being disclosed to the requester, or
- if these options are not possible, whether it is reasonable in the circumstances to disclose the images to the individual making the request in any case.

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

- when the request was made and by whom
- what factors were considered in deciding whether to allow access to any third party images
- whether the requester was permitted to view the footage, or if a copy of the images was provided, and in what format.

Requesters are entitled to a copy in permanent form. If a permanent copy is requested, this should be provided unless it is not possible to do so, or it would involve disproportionate effort. (For example, it may be acceptable to allow a requester to view footage which contains third party images, but not to provide a permanent copy.)

7. Third party access

7.1. Third party requests for access will usually only be considered, in line with the data protection legislation, in the following categories:

- from a legal representative of the data subject (letter of authorisation signed by the data subject would be required)
- from law enforcement agencies including the police
- disclosure required by law or made in connection with legal proceedings
- HR staff responsible for disciplinary and complaints investigations and related proceedings, and
- Staff employed by our contractors responsible for disciplinary and complaints investigation and related proceedings concerning their own staff.

7.2. Where images are sought by other bodies/agencies, including the police, with a statutory right to obtain information, evidence of that statutory authority will be required before CCTV images are disclosed.

7.3. The DPO will consider disclosing recorded images to law enforcement agencies once a form certifying that the images are required for one of the following reasons has been received:

- an investigation concerning national security
- the prevention or detection of crime, or
- the apprehension or prosecution of offenders,

and that the investigation would be prejudiced by failure to disclose the information. The DPO will also need to take into account the guidance in BSB's "Requests for Information from the Police" (Ref: ROD09), as necessary.

7.4. Where third parties are included in images as well as the person who is the focus of the request, the same considerations need to be made as in the case of subject access requests.

7.5. Every disclosure of CCTV images (including where authorised persons are given access to view footage in GCB's office) is recorded in the CCTV Operating Log Book and contains:

- the name of the police officer/other relevant person receiving the images
- brief details of the images captured by the CCTV including the date, time and location of the footage/images
- the purpose for which they will be used
- the crime reference number where relevant, and
- date and time the images are handed over to the recipient.

8. Complaints procedure

8.1. Any complaints relating to the CCTV system should be directed in writing to the Head of Facilities and Property promptly and in any event within seven days of the date of the incident giving rise to the complaint. A complaint will be responded to within a month of the date of its receipt. Records of all complaints and any follow-up action will be maintained by the relevant office.

8.2. Complaints in relation to the release of images should be addressed to the DPO. These will be responded to promptly and, in any event, within 30 days of receipt. They will be dealt with in accordance with the provisions of the UK GDPR and the Data Protection Act 2018 (or any successor legislation).

Appendix 1

LIA for operating CCTV in the office

Please see the Information Commissioner’s [guidance on Legitimate Interests](#)

The General Council for the Bar operates CCTV cameras at the entrances to each of its office floors. Other CCTV cameras operate in other locations in the office which are operated and controlled by the building’s landlord.

Part 1: Purpose test (identifying a legitimate interest)

We need to assess whether there is a legitimate interest behind the processing.

- Why do you want to process the data?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are the benefits that you have identified?
- What would the impact be if you couldn’t go ahead with the processing?
- Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice?
- Are there any other ethical issues with the processing?

CCTV is operated in the building primarily for security and safety reasons, to protect staff, visitors, the premises and the computer servers. This could include aiding the investigation of accidents or incidents. Occasionally, CCTV images may also be used in HR disciplinary investigations involving our own staff.

The primary beneficiaries are our staff, by enabling them to be secure. The presence of the CCTV will also help to give a perception of security and safety. Where HR are investigating a disciplinary matter where there has been a dispute between members of staff, the processing will benefit the injured party in the dispute.

The wider public benefits are that the processing helps to ensure the safety of anyone visiting the building, and in helping to keep the building secure, this adds to the overall security arrangements the GCB have in place to ensure security of personal data held by the organisation more widely.

The benefits are important in ensuring the safety and wellbeing of staff and visitors, and giving reassurance to those people that their safety is a priority. It is also important to help protect the building and computer system as described above.

If we didn’t go ahead with this processing, safety and security within the building may be compromised. Business continuity and security of personal data may be compromised.

We may not be able to prove allegations made against staff in relation to health and safety or potential accident or disciplinary claims without CCTV evidence.

There are no ethical issues as our use of CCTV complies with the ICO's Guidance on Video Surveillance (undated) and the Biometrics and Surveillance Camera Commissioner's 12 guiding principles in their Surveillance Camera Code of Practice (2021). The system does not use wifi or transmit images over the internet. The device that stores the images is located in the locked comms room.

Part 2: Necessity test

We need to assess whether the processing is necessary for the purpose we have identified.

- Will this processing actually help you achieve your purpose?
- Is the processing proportionate to that purpose?
- Can you achieve the same purpose without the processing?
- Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

The processing will help us achieve our purpose for the reasons set out above, and the processing is proportionate in that we only have cameras where needed for this purpose. We cannot achieve the same purpose without this processing, or by doing any less processing.

Part 3: Balancing test

*We need to consider the impact on individuals' interests, rights and freedoms and assess whether this overrides the legitimate interest we have identified. First, use the DPIA screening form to see if we need to carry out a Data Processing Impact Assessment to assess the risks in more detail. **If a DPIA is required, this can take the place of this LIA.***

Nature of the personal data

- Is it special category data or criminal offence data?
- Is it data which people are likely to consider particularly 'private'?
- Are you processing children's data or data relating to other vulnerable people?
- Is the data about people in their personal or professional capacity?

Data could be sensitive, including special category data and criminal offence data, depending on the context, for example, if footage/images were to be used in connection with a disciplinary offence. Otherwise, it is not sensitive or particularly private. For our employees, it is only data in their professional capacity and, generally speaking, this will be the same for visitors. We are only recording images of staff and visitors to the building, in public areas. Recordings are available on a live feed and kept for 30 days. After that period they are overwritten. This is considered the shortest reasonable time to allow for requests for the images to be made and dealt with, for example, if an accident has taken place and it is necessary to review what happened.

We do not process children's data, unless they visit the office. This is unlikely given the nature of our activity. Occasionally staff may bring their children to the office, but they are

aware of the CCTV operation. It is unlikely any visitors to the office are vulnerable, but any vulnerability should not be affected by the operation of the CCTV system.

Reasonable expectations

- Do you have an existing relationship with the individual?
- What's the nature of the relationship and how have you used data in the past?
- Did you collect the data directly from the individual? What did you tell them at the time?
- If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
- How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
- Is your intended purpose and method widely understood?
- Are you intending to do anything new or innovative?
- Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation?
- Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

Our relationship with the individual is either as employer (and so responsible for the safety of our staff) or organisation responsible for the safety of visitors, most of whom we have an existing relationship with, eg committee and board members.

No data is obtained from third parties – it is recorded in the office and kept for the minimum reasonable time of 30 days. There is nothing new or innovative about this processing.

We believe our intended purpose and method is understood. We display notices as appropriate, and such systems are common in office buildings.

Likely impact

- What are the possible impacts of the processing on people?
- Will individuals lose any control over the use of their personal data?
- What is the likelihood and severity of any potential impact?
- Are some people likely to object to the processing or find it intrusive?
- Would you be happy to explain the processing to individuals?
- Can you adopt any safeguards to minimise the impact?

The impact on the individual is only likely to be beneficial unless they have done something wrong, such as displaying aggressive behaviour, while being filmed. It can be helpful to review footage if an accident has happened, for example.

Under normal circumstances, the impact is likely to be very small. It will only have a significant impact if the person filmed has done something wrong (see above), they are an intruder or someone else has acted inappropriately towards them. If CCTV images provide evidence of a disciplinary offence, disciplinary measures could be taken against the offender; or evidence of an accident, there could be compensation claims.

No-one has objected to the processing to date. We are happy to explain our processing - we include information on our use of CCTV in our privacy notices, and we have a CCTV Policy.

The impact is already minimised in that CCTV is only operating in the most vulnerable locations and the recordings are kept for a minimum period.	
Can we offer individuals an opt out?	Yes / No

Making the decision

Use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

Can you rely on legitimate interests for this processing?	Yes / No
Do you have any comments to justify your answer? (optional) We have also completed a DPIA on CCTV operation in the office in May 2022.	
LIA completed by	Catherine Shaw, Director of HR (Revisions, Andy Curtis, Head of FM)
Date	October 2018, revised Nov 2019, Jan 2020, May 2022
Submitted to DPO (date)	June 2023 (latest version)

The DPO will keep a record of this LIA and any accompanying DPIA. The LIA should be kept under review and be refreshed if there is a significant change in the purpose, nature or context of the processing.

Appendix 2

Checklist for users of limited CCTV systems

This CCTV system and the images produced by it are controlled by Andy Curtis, Head of Facilities and Property, who is responsible for how the system is used.

We (The General Council of the Bar) have considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of individuals and the security of premises. See our Legitimate Interests Assessment for Operating CCTV. It will not be used for incompatible purposes, and we conduct regular reviews of our use of CCTV to ensure that it is still necessary and proportionate. We conduct an annual review of our use of CCTV.

	Notes	Checked (date)	By	Date of next review
Our system is processing footage of identifiable individuals and is processing personal data. We have registered as a controller and paid the relevant data protection fee to the ICO.		13/6/23	DPO	June 2024
There is a named individual who is responsible for the operation of the system.	Andy Curtis, Head of Facilities and Property	13/6/23	DPO	June 2024
The problem we are trying to address has been clearly defined. We regularly review our decision to use a surveillance system.	See our Legitimate Interests Assessment for Operating CCTV	13/6/23	DPO	June 2024
We have identified and documented an appropriate lawful basis for using the system, taking into consideration Articles 6, 9 and 10 of the UK GDPR and relevant schedules of the DPA 2018.		13/6/23	DPO	June 2024
Our system produces clear images which we can easily disclose to authorised third parties. For example, when law enforcement bodies (usually the police)	System supplied by BlueSky	14/6/23	DPO & AC	June 2024

require access to investigate a crime.				
Cameras have been sited so that they provide clear images.	Yes	14/6/23	AC	June 2024
We have positioned cameras in a way to avoid any unintentional capture of images of private land or of persons not visiting the premises.	No exterior cameras	13/6/23	DPO & AC	June 2024
There are visible signs showing that CCTV is in operation. Contact details are displayed on the signs if it is not obvious who is responsible for the system.	Yes, and contact details now included	14/6/23	DPO & AC	June 2024
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	Stored on Digital Video Recorder linked to Network. Only access by Facilities staff	14/6/23	AC	June 2024
The recorded images will only be retained long enough for any incident to come to light (eg for a theft to be noticed) and the incident to be investigated.	Images retained for 30 days – but can be extended if further investigation needed, or images can be downloaded	14/6/23	AC	June 2024
Except for law enforcement bodies, images will not be provided to third parties.	Under RIDDOR images need to be available to insurance co's too (covered by 'Disclosure required by law')	14/6/23	AC	June 2024
Our organisation knows how to respond to individuals making requests for copies of their own images, or for images to be erased or restricted. If unsure the controller knows to seek advice from the Information	Yes, as long as request made within 30 days. Can easily isolate frames and save to encrypted zip file.	14/6/23	AC & DPO	June 2024

Commissioner as soon as such a request is made.				
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	Planned preventive maintenance, done quarterly	14/6/23	AC	June 2024

Please keep this checklist in a safe place until the date of the next review.

AC – Andy Curtis, Head of Facilities Management

DPO – Hilary Pook

June 2023