Parliamentary Security Camera Policy

Introduction

1. Security cameras are employed in various parts of the Parliamentary estate. They are a vital part of the security system for the estate and make an important contribution to public safety and security by helping to protect both people and the extremely valuable and important heritage and property that are contained within the estate.

2. The use of security camera systems within the Parliamentary estate is carefully regulated so that they contribute to the aims for which they are installed and do not become intrusive and a limitation on the freedom or legitimate activities of those visiting or working within Parliament. The purpose of this policy is threefold:

a. to set out the Parliamentary policy for the control, use and regulation of surveillance systems within the Parliamentary estate;

b. to ensure that individuals and wider communities are aware of the purposes and general characteristics of the security camera systems that are installed;

c. to explain the provisions for the use of imagery captured by security camera systems.

3. This policy has been developed using the guidelines laid down in the Home Office Surveillance Camera Code of Practice of June 2013.[1]

4. Security camera systems within Parliament are only used where they are:

- in pursuit of a legitimate aim
- necessary to meet a pressing need
- proportionate
- effective
- compliant with any relevant legal obligations and codes (whether formally applicable to Parliament or not).[2]

5. Security camera systems are used in public areas of the Parliamentary estate[3] and areas considered vulnerable to intrusion from which the general public are normally excluded. Moreover, security camera systems are only deployed where achieving the same effects by other means is not practical or cost effective or where there is a Health and Safety need.[4]

Scope

[1] While section 33 of the Protection of Freedoms Act 2012 does not apply to Parliament (and therefore neither does the Code), the Parliamentary authorities seek to act, so far as possible, as if it did.

[2] This policy takes into account the guidelines set out in the Home Office Surveillance Camera Code of Practice 2013 as well as relevant provisions of the UK GDPR, Data Protection Act 2018, the Protection of Freedoms Act 2012 and the Investigatory Powers Act 2016.

[3] "Public place" has the meaning given by Section 16(b) of the Public Order Act 1986 and is taken to include any highway and any place to which at the material time the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission.

[4] Eg, by having the same area monitored by a Security Officer or Doorkeeper or pass activated access control.

6. For the purposes of this policy, any reference to the Parliamentary estate includes the outbuildings connected with either House as well as the Palace of Westminster and any other spaces which come under the supervision of the Parliamentary authorities. This code applies to the use of overt security camera systems and includes:

- CCTV systems deployed in public areas
- under-vehicle camera systems
- automatic number plate reading systems
- X-ray systems at entry points
- systems for recording or viewing visual images for security purposes
- systems for storing, receiving, transmitting, processing or checking the images or information obtained by the systems above.

The policy does not include camera systems not owned by or under the control of the Parliamentary Authorities such as news broadcasters, cameras and video recordings made by members of the public, Members of either House, contractors and the police, notably body worn video.

7. Responsibility for images captured by these systems is the responsibility of the individual or organisation taking the images and, in the case of organisations, subject to their controls on use and release of data. Before permission is given to install or use such systems operated by organisations contracted to Parliament the system operator, acting as the relevant authority, will review the control and data release processes operated by that organisation to ensure they comply with the provisions of this policy.

Responsibility and Accountability for the Parliamentary CCTV System

8. Responsibility and accountability of the Parliamentary CCTV system is vested at a number of levels and as mentioned in Para 3, conforms to the principles set out in the Home Office Surveillance Camera Code of Practice.

a. Ownership of the Parliamentary security camera policy and associated regulations is vested jointly in the Clerk of the House and the Clerk of the Parliaments as the Corporate Officers who, for the purposes of the General Data Protection Regulation (UK GDPR), are Controllers of personal data processed on behalf of the House of Commons and House of Lords respectively.

b. Oversight of the Security Camera policy and its general operation is undertaken by the Serjeant at Arms in the House of Commons and Black Rod in the House of Lords. They act as if they were "relevant authorities" on behalf of the Corporate Officers for the purpose of section 33 of the Protection of Freedoms Act 2012.[5] Within this role, they control the use or processing of images or other information obtained from the system.

[5] "Relevant authority" has the meaning given by Section 33(5) of the Protection of Freedoms Act 2012.

c. The operation of the Parliamentary CCTV security cameras and the processes and codes of practice that govern its use is the responsibility of the Director of Security for Parliament. Within the meaning of the Home Office Surveillance Camera Code of Practice 2013, they act as the "System Operator" and "System User"; ie, the head of the staff who operate the system and whose employees have access to live or recorded images or other information obtained from the CCTV system. As such, they coordinate the decisions relating to the deployment of the security camera system, define its operating parameters and liaise closely with Black Rod and the Serjeant at Arms along with the legal and data protection staffs in both Houses to ensure that a balance is maintained between the security and other purposes of the system and privacy considerations.

System Capabilities

9. The capabilities of the Parliamentary security camera systems are subject to development and change. Currently they comprise a network of CCTV cameras covering internal and external areas of the Parliamentary estate (including the roof, approaches to access points and areas considered vulnerable to intrusion), X-ray systems at pedestrian entrances, under-vehicle cameras at vehicle entry gates and equipment associated with recording, copying and transmitting images and information derived from the camera systems. The system also has access to camera imagery from the network of Metropolitan Police Service ("MPS") security cameras and traffic cameras in the wider environs of Westminster. Capabilities include:

a. Staffed monitoring points at various locations around the Parliamentary Estate and its outbuildings

b. Recording equipment capable of capturing the images from all CCTV cameras on the Parliamentary Estate simultaneously.

Provisions for the Use of Security camera systems within the Houses of Parliament

10. The Parliamentary security camera system seeks to strike a balance between meeting the need for security and avoiding the possibility of intruding into an individual's privacy. Much of this requires subjective judgement and thus, decisions on the deployment and use of security camera systems are subject to consideration by Members through the Consultative Panel for Parliamentary Security (CPPS) as part of the system for ensuring that appropriate safeguards are in place, and to agreement by the Clerks of both Houses.

11. **Deployment, Operation and Exploitation of Security Cameras**. The deployment, operation and exploitation of security cameras within Parliament adhere to the broad provisions set out below. These enable an appropriate 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.

a. **The purpose of the Security Camera System within Parliament**. The security camera systems operating within the Palace of Westminster are deployed primarily to:

i. support the security of the Houses of Parliament
ii. prevent unauthorised access to the Parliamentary Estate or parts thereof
iii. help protect it from attack, protest or disruption by individuals acting maliciously, illegally or outwith the rules and regulations of both Houses.
iv. assist in ensuring public order and safety

The security camera network will also aid the prevention, detection, investigation and prosecution of crime, including damage to property. It will also enable internal investigations to establish the facts of events which may constitute misconduct by staff and/or visitors or breaches of Health and Safety practices and codes. The ability to record and review footage and images is a necessary part of the capability of the system because the end users are likely to be the police and the criminal justice system and the Parliamentary authorities. Any proposed extension to the purposes set out above will be subject to consultation with the CPPS.

b. **Respect for effect of Security Camera Systems on individuals and their privacy.** Security camera systems in the Parliamentary Estate are only used in areas that can reasonably be regarded as public places or where there is considered to be a particularly high risk of intrusion or vulnerability. They are not used where there is a reasonable expectation of privacy. In addition:

i. Areas under security camera coverage are routinely reviewed to ensure the capability meets the purposes set out in Para 10a.

ii. Security camera systems do not record conversations.

iii. Video analytics, where introduced, are only used when it is clearly justified and proportionate in meeting a stated purpose. Its use for this purpose is subject to approval from the Director of Security for Parliament, the Serjeant at Arms or Black Rod or their nominated representatives.[6] Where there is any issue involving Members, or if there is any issue of political sensitivity, the authority of the relevant Clerk will be sought.

iv. When using or releasing images for the purposes set out in Para 10a, account is taken of the privacy impact on non-involved individuals and where possible, feasible and proportionate, the identity of these individuals is protected.

v. When improvements to existing Security camera systems are being considered (including replacement of existing ones) or when CCTV monitoring is extended into new areas of the Parliamentary estate, a privacy impact assessment is conducted to ensure that the purpose of the system is justifiable. Consultation with those most likely to be affected is also conducted through the CPPS.

c. **Transparency of use.** Those areas subject to CCTV coverage are clearly signposted. The signs also make it clear why and by whom the area is being monitored. This does not apply to X-ray and under-vehicle camera systems as the visual nature of the equipment is obvious. The privacy notices

[6] Nominated representatives are the Deputy Parliamentary Security Director, the Yeoman Usher and the Serjeant at Arms Access Manager.

published on the Parliament website[7] must specify matters such as how we process any personal data in images captured by CCTV, the legal basis for the processing and the rights of the data subjects. Other components of transparency include:

i. Complaints. Any complaints relating to the deployment or operation of the CCTV system should be made within 3 months of the date on which the complainant became aware of the occurrence complained of. Complaints should initially be addressed to the Serjeant at Arms Department in the House of Commons or Black Rod's Department in the House of Lords for informal resolution. Should informal resolution not be possible, then the matter should be made subject to a formal complaint which should be submitted to the Clerk Assistant in the House of Commons or the Reading Clerk in the House of Lords. Once an investigation into the complaint has been completed, a response will be sent to the complainant. This response will include information on other regulatory bodies who may have jurisdiction in the matter such as the Information Commissioner.

ii. Criminal Offences. Should, in the course of an investigation, it become apparent that a criminal offence may have been committed, then the investigator will inform the Parliamentary Authority under whose supervision the investigation is being conducted and, after consultation with them, refer the matter to an appropriate body such as the Police or the Information Commissioner for any offences under the Data Protection Act 2018.

d. **Policy for the Use and Operation of the Parliamentary CCTV System.** The following conditions apply to the operation and use of the Parliamentary CCTV system.

i. CCTV operators are designated and trained by the Parliamentary Security Directorate to operate equipment. Non-designated personnel may also monitor CCTV systems on an as-required basis for specific purposes but when this happens, they will do so under the overall supervision of a designated operator. In exceptional situations such as illness or emergencies, non-designated operators may operate systems but these are logged and the reasons recorded.

ii. A record is maintained of which staff have access to the CCTV recording system at any given time.

e. **Storage of images and information**. Images and information derived from the Parliamentary security camera systems is stored to assist in reviewing incidents, to assist in reconstructing events and to enable lessons to be derived. They are also used to facilitate the investigation of public order and safety incidents, criminal acts or misconduct by staff, visitors or other persons on the Parliamentary Estate. Information from the systems is used, where necessary, for evidential purposes in criminal prosecutions or when dealing with internal disciplinary matters. As a general principle, images are to be kept "in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed"[8] and as a general rule, are usually deleted after 28

[7] In accordance with Article 13 of the UK GDPR.

[8] This is a requirement of UK GDPR (Article 5(1)(e)). Further guidance on this is contained in the ICO CCTV code of practice

days.[9] However, it may be appropriate to retain the image or information for a longer period where it is needed:

i. for evidential purposes, for example to investigate a crime or an accident;

ii. to establish patterns of behaviour or routines of individuals suspected of hostile intent or serious misconduct;

iii. for training purposes or to illustrate wider lessons captured on the cameras provided all personal information is redacted;

iv. for the purposes of responding to a data subject access request made under Article 15 of the UK GDPR (Re. para. 9. g. iii.) or a request made under the Freedom of Information Act 2000 (Ref. para. 9. g. v).

f. **Access to retained images and information**. The disclosure of images and other information obtained from the Parliamentary CCTV system is allowed but release must be consistent with the purposes for which the CCTV system is used and which are set out in Para 10a. Exceptionally, the relevant authorities[10] will give authority to disclose information to third parties other than the System Operator or System User, for example, to prevent the commission of a crime or apprehend persons who have committed a crime, conducted an act of disorder or damage to property or misconduct by staff, visitors or other persons on the Parliamentary Estate. In these cases, the System Operator will ensure that release meets the legal requirements. Additionally:

i. Judgements about disclosure are made by the relevant authorities who have the discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or a data subject access request under Article 15 UK GDPR. If applicants are dissatisfied with the decision of the relevant authority, they may refer the application to the Controllers in each House (ie, the Clerks) for review.

ii. Once the images and information have been disclosed the receiving body, such as the police, becomes responsible for their copy of that image. Following release, it is then the recipient's responsibility to comply with any legal obligations and the Home Office Code of Practice in relation to any further disclosures.

iii. Individuals can request images and information about themselves through a subject access request[11] under Article 15 of the UK GDPR (right of access by the data subject). Each application will be assessed on its own merits and general 'blanket exemptions' will not be applied. However, in considering a request made under Article 15 of the UK GDPR, one or more of the exemptions set out in Schedule 2 to the Data Protection Act 2018 may apply including in particular the following:

Personal data processed for any of the following purposes:-

[9] This period is kept under review.

[10] See paras 7b and 10b iii

[11] Detailed guidance on this and matters such as when to withhold images of third parties caught in images is included in the ICO CCTV code of practice.

i) The prevention or detection of crime

ii) The apprehension or prosecution of offenders

are exempt from [the subject access provisions] *in any case 'to the extent to which the application of those provisions to the data would be likely to prejudice any of* [those matters]'.

iv. Within the statutory framework provided under the Criminal Procedures and Investigation Act 1996, disclosure can also be made to defendants of material which the prosecution would not intend to use in the presentation of its own case (known as unused material). Disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the controller by Article 15 of the UK GDPR (known as subject access).

v. Requests for information from public bodies (including each House of Parliament) may be made under the Freedom of Information Act 2000.[12]

g. **Security measures to safeguard against unauthorised access and use of CCTV images and information**. The release of images and information for use as evidence in legal or disciplinary proceedings is subject to careful security safeguards in order to comply with legal obligations and to help foster public confidence. Images are only released after a formal request, with an auditable justification, has been made and authority has been given by either Black Rod, the Yeoman Usher as their nominated deputy, the Serjeant at Arms or their nominated deputy. Exceptionally, where release is time critical to control an ongoing situation, prevent crime or apprehend suspects, the Control Room Supervisor or PSD Duty Operations Manager may make the authorisation but must justify and seek confirmation of their decision from the Yeoman Usher or SAA Access Manager at the first opportunity. Images and information will only be used for the purposes set out in Paragraph 10a and due account will be taken of privacy considerations relating to non-involved individuals and if necessary, conditions imposed. The release or disclosure of data for commercial or entertainment purposes is specifically prohibited. No release involving members will be agreed without consulting the relevant Clerk, unless in cases of urgency.

h. **The use of the Parliamentary CCTV system to support public safety and law enforcement through the processing of images and information of evidential value**. Part of the effectiveness of the Parliamentary security camera system is its capability to capture, process, analyse and store images and information at a quality which is suitable for public safety, crime prevention, detection, investigation and prosecution. The procedural and technical safeguards help ensure the forensic integrity and reliability of recorded images and information, including any metadata (e.g. time, date and location). It also ensures that the rights of individuals recorded by the Parliamentary security camera system are protected and that the material can be used as evidence in court. In order to ensure that this capability is maintained, any upgrades to existing systems or new security camera systems ensure that:

[12] Ibid.

i. The images and information from the security camera systems are exportable when requested by a law enforcement agency.

ii. The export of images and information is possible without interrupting the operation of the system.

iii. The exported images and information are in a format which is interoperable and can be readily accessed and replayed by a law enforcement agency.

iv. The exported images and information preserve the quality of the original recording and any associated metadata (e.g. time, date and location).

i. **Maintenance of CCTV records, information and databases**. Use of technologies such as Automatic Number Plate Readers or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by others are only introduced once an assessment has been made to ensure the underlying data are fit for purpose. This not only helps ensure the reliability, accuracy and integrity of data but it protects the information by limiting its use to the purposes for which it was intended.