Home Office

Detention Services Order 04/2017

Surveillance Camera Systems

August 2025

This publication is available at www.gov.uk/government/collections/detention-service-orders

Any enquiries regarding this publication should be sent to us at DSOConsultation@homeoffice.gov.uk

Contents

Document Details

Process: To provide information for staff and contracted service providers on the use of surveillance camera systems, including the management and security of data.

Publication Date: May 2024 (updated August 2025)

Implementation Date: February 2018 (reissued May 2024)

Review Date: May 2026

Version: 2.2

Contains Mandatory Instructions

For Action: All Home Office staff and contracted service providers operating in immigration removal centres (IRCs), pre-departure accommodation (PDA), and short-term holding facilities (residential and non-residential), in addition to escorting suppliers.

For Information: N/A

Author and Unit: Dean Foulkes, Detention Services.

Owner: Michelle Smith, Head of Detention Operations

Contact Point: Detention Services Orders Team.

Processes Affected: All processes relating to the use of surveillance camera systems, including the management and security of data.

Assumptions: Surveillance camera system operators will have the necessary knowledge of the legislation that applies to its use.

Notes: N/A

Instruction

Introduction

1. This Detention Services Order (DSO) provides operational guidance for all staff working in immigration removal centres (IRCs), pre-departure accommodation (PDA) and short-term holding facilities (STHFs) (residential and non-residential) in addition to escorting staff, on the use of surveillance camera systems.

2. This instruction **does not** apply to Residential Holding Rooms (RHRs).

3. For this guidance, "centre" refers to IRCs, STHFs and the PDA.

4. Two separate Home Office teams operate in IRCs:

    - Detention Services Compliance Team (Compliance team)
    - Detention Engagement Team (DET)

    The **Compliance teams** are responsible for all on-site commercial and contract monitoring work. The **DETs** interact with individuals face-to-face on behalf of caseworkers within the IRCs. They focus on communicating and engaging with people detained in IRCs, serving paperwork on behalf of caseworkers, and helping them to understand their cases and detention.

    There are no DETs at RSTHFs. Some of the functions which are the responsibility of the DET in IRCS, are carried out by the contracted service provider in RSTHFs and overseen by the International and Returns Services (IRS) Escort Contract Monitoring Team (ECMT). In the Gatwick PDA, the role of detained individual engagement is covered by the local Compliance Team.

Definition of a surveillance camera system

5. Surveillance, for the purposes of the Regulation of Investigatory Powers Act 2000 (RIPA) includes monitoring, observing, or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained (see DSO 02/2015 Regulation of Investigatory Powers Act 2000 (RIPA).

6. A surveillance camera system is an umbrella term for any system used for the recording and retaining of visual images for surveillance purposes, which includes:

- A body worn camera (BWC). This is a camera worn on the body in an overt capacity by a user for the primary purpose of recording video and audio material.
- A hand-held camera (HHC). This is a camera with limited features used for recording video and audio material by hand.
- Closed circuit television (CCTV). This is the use of overt video cameras to transmit images to a specific limited number of televisions on the same network or circuit, primarily used for surveillance and security purposes.

Policy

7. Surveillance camera systems are used to monitor and record activity within IRCs and during escort for the safety and security of staff, detained individuals, and the public. Recorded footage can help assure that the highest professional standards are being maintained by staff and provides beneficial evidence in the investigation of complaints and criminal investigations/ procedures, in addition to inquests and serious incident reviews.

8. The use of surveillance cameras and data processing must be in accordance with all relevant legislation including the Data Protection Act 2018 [1] (DPA), the Regulation of Investigatory Powers Act 2000 (RIPA)[2] the Human Rights Act 1998[3] Protection of Freedoms Act 2012[4], where applicable.

9. Article 6 of the UK General Data Protection Regulation (GDPR,) stipulates there must be a lawful basis for processing personal data. Processing includes but is not limited to, the recording, organising, and restructuring of data, storing data, and creating a record. It is part of the Home Office's duty as the Data Controller to fulfil this legal obligation under the UK GDPR. Other parties operating the surveillance systems and processing the data on behalf of the Home Office (private contractors and escort suppliers) will be acting as Data Processors under the UK GDPR.

10. The use of surveillance cameras and management of data should also show due regard to the Home Office surveillance camera code of practice[5] and comply with the Home Office personal information charter[6]. In addition, when a contracted service provider is considering the introduction of new surveillance camera systems, or

[1] https://www.legislation.gov.uk/ukpga/2018/12/contents

[2] http://www.legislation.gov.uk/ukpga/2000/23/contents

[3] http://www.legislation.gov.uk/ukpga/2000/36/contents

[4] http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

[5] https://assets.publishing.service.gov.uk/media/619b7b50e90e07044a559c9b/Surveillance_Camera_CoP_Accessible_PDF.pdf

[6] https://www.gov.uk/government/organisations/home-office/about/personal-information-charter

reviewing the use of any existing surveillance camera systems in a centre, the contracted service provider must complete a data protection impact assessment (DPIA), in line with the Surveillance Camera Commissioner's guidance, to assess the impact of the system on people's privacy (whether a detained individual, staff or visitor). This should include consideration of whether its intended use has a lawful basis and is justified, necessary and proportionate.

Procedures

11. Under Article 5(1)(f) of the UK GDPR, Data Controllers must have appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data.

12. The contracted service provider as the data processor, must have a local policy in line with this DSO on the use of surveillance camera systems, which must clearly justify the need for both video and audio recording (for example gathering evidence or complaints management). Any consideration of recording audio alongside video recording must have a higher level of justification than video recording alone. The DPIA and both the Surveillance Camera Commissioners self-assessment tools[7] on the code of practice and body worn video should be completed when developing or revising the centre's local policy, with the results provided to the local Compliance team on request. The final policy must be agreed by the local Compliance Delivery Manager in consultation with the Detention Services Security Team (DSST) and lead Detention Services Data Protection Practitioner (DPP) before implementation. In addition, the local Compliance Delivery Manager must review and agree any substantive revisions to the centre's local policy on an annual basis. Any issues arising with approval of the local policy should be escalated to the Head of Detention Operations for a final decision.

13. Each local policy on the use of surveillance cameras and the management of surveillance camera data must include the following details:

    - why the data is needed and how it will be processed.
    - what processes are in place to avoid collecting too much or irrelevant information
    - any restrictions on access to data and other security measures for maintaining the security of the footage
    - instances when cameras should be switched on/used e.g., during uses of force, serious incidents, room searching or interactions that staff consider involve a risk to safety

[7] https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-self-assessment-tool

- the procedures for sharing data with other organisations
- the procedures for notifying detained individuals and visitors that surveillance camera systems are in use, and why they are deemed necessary – including the use of surveillance systems during the removal process
- data retention periods and deletion processes - in accordance with paragraphs 60-70
- audit and assurance processes in connection with the use of surveillance cameras must include the completion and recording of quarterly audits to ensure that information held, both personal and procedural, can be accounted for.

14. Contracted service providers must inform detained individuals upon induction into the centre that there is surveillance camera equipment in operation within the establishment and explain the circumstances in which each type of equipment is used.

15. Internal and external signage should be displayed at each entrance to the centre, notifying detained individuals and visitors that surveillance cameras are in use and visual and audio recording may be carried out. Internal notices should also detail the process for accessing material regarding those subject to surveillance, including an IRC contracted service provider contact telephone number for those in detention and visitors to use in case of query or complaint. Signage should also be clear in the Care and Separate Unit (CSU) area as well as areas where BWCs may be frequently used.

16. Surveillance cameras should not be used in toilets, showers, bedrooms, healthcare facilities (excluding waiting rooms that do not compromise any healthcare consultation/interactions and subsequent confidentiality) or areas primarily used for the searching of persons, unless there are exceptional circumstances (e.g. first responders to a serious incident) where their use is strictly necessary to gather evidence, and there is no other reasonable means of gathering the necessary evidence. If it becomes apparent to contracted service provider staff during an incident (in any of the locations) in which surveillance cameras are being used, that the incident is not considered serious, surveillance cameras must then be turned off.

17. Where surveillance cameras have been used during an incident, their use should be authorised by the Detention Services duty manager (grade SEO or above) and the justification recorded in writing in local contracted service provider records, however the use of surveillance cameras should not delay a response to an incident, for example, responder staff should not attempt to replace faulty surveillance equipment before attending a live incident.

18. If it is not possible to obtain duty manager authorisation, the member of staff recording the incident should state out loud the justification for its use in these areas to the camera, so that there is a formal record of the decision.

19. Surveillance cameras may not be used inside a room or search area during a full search being carried out on a detained individual. Surveillance camera systems (such as BWCs or HHCs) may however be used for the sole purpose of gathering audio evidence of the interactions during a full search, however, this must be explained to the detained individual prior to the start of the full search and the camera operator must identify themselves on the audio recording. Camera operators must ensure they remain outside the room, but appropriately placed to ensure audio surveillance is captured.

20. BWCs should be activated in all situations where force is required to be used, but where the detained individual is in a state of undress, the BWC must not be pointing at the individual whilst he is being covered as quickly as possible. This will ensure that any sound is recorded with the visual footage only interrupted for a very short period.

21. Cameras may be used by staff to record briefing or debriefing sessions before or following an incident. Recorded briefings must never be a replacement for written statements or incident reports. The preparation of any briefing or debriefing transcripts does not mean that any recorded footage can be deleted.

22. Where possible, all surveillance cameras in use should have a built-in memory and the recorded footage should be encrypted.

23. Where planned interventions/relocations occur, staff must consider their location when recording and captured footage must provide sufficient coverage of the incident/event.

Body Worn Cameras (BWC)

24. Contracted service providers must have in place effective procedures to manage BWC assets, which should accurately record who a device is assigned to, the location of the device and its operational status. The procedures used to manage BWC assets must be fully auditable, and records of the use of each camera or of each officer assigned to use the BWC must be made available to the local Compliance manager or Home Office Security staff on request.

25. When involved/responding to any incident, BWCs must be activated without exception and the user should commence recording at the earliest opportunity. This includes when staff enter bedrooms to safeguard staff and residents in the event of any allegation of inappropriate conduct. The member of staff recording the incident should state out loud the reason for turning on the BWC; In the event he/she is reasonably unable to do so, they must ensure they fulfil this requirement upon conclusion of the incident. This ensures that there is a formal record of the decision to use the BWC and notifies detained individuals and staff in the area that they are being recorded by both video and audio surveillance (if applicable). Staff dressed in personal protective

equipment (PPE) should also identify themselves to the camera, ensuring that their protective helmets (with front and back facing numbers, for the purpose of staff identification) are visible - before carrying out any actions. This will ensure that they are identifiable when incidents are reviewed.

26. Recordings should be uninterrupted from the beginning until the end of the incident, unless a lengthy incident occurs where there may be periods of inactivity, in which only relevant parts of the incident may be filmed. The camera user should cease recording when either the incident has concluded or it is no longer felt justifiable, proportionate, or necessary to continue to record. The operator must document and justify the decision to stop recording in their written statements or reports following the incident. If a request has been made to cease recording, it is for the camera operator to decide if this is justifiable or if the recording should continue. Should the operator continue recording, the justification must be stated to the camera. Once the recording has ceased, the data should be downloaded from the device at the end of the shift or earlier if possible. Where the spontaneous use of a BWC has occurred, a post-incident debrief must be recorded.

27. BWCs should be used:

    - When spontaneous use of force is required against a detained individual(s);
    - On a planned relocation where the use of force is assessed as a possibility – see also paragraph 30
    - If the wearer believes the interaction presents, or is likely to present, a risk to the safety of the wearer, other members of staff, detained individual or other persons present
    - If the wearer considers the use of BWC to be a necessary and proportionate means of recording any other interaction or event
    - When available, consideration should be given by officers to activating a BWC at a detained individual's request
    - When interacting with detained individuals in the CSU (from the time the door is opened).

28. Where BWCs should routinely be used as per paragraph 27 but have not been used, records must be kept of the reasons why.

29. BWCs must not be used to:

    - Film covertly
    - Record general work practices

- Record interactions between any persons without specific cause
- Record the conduct of any type of search of a person (see para 19 for exemptions to this)

30. In accordance with DSO 07/2016 Use of Restraint(s) for Escorted Moves – All staff, all use of force paperwork must be completed by each officer, independently of other staff involved. Ideally, reports should be completed as soon as possible after the incident. Failure to do so may leave staff/managers/contracted service providers open to serious allegations, disciplinary action, and possible litigation. Once completed, all use of force reports must be submitted to the local Home Office Compliance Team as soon as possible and no later than 24hrs following the incident. As part of this initial paperwork, Annex A (a form officers utilise to detail the type of force they engaged in and indicate the technique utilised), should be completed and submitted within 72 hrs. In exceptional circumstances, use of force reports may be provided up to a period not exceeding 72hrs, however contracted service provider staff must advise the Compliance Team of this and reasons for exceeding the initial 24hr period.

31. When surveillance cameras are used to record an incident involving the use of force, the use of force report must contain a log or reference number of the footage in accordance with paragraphs 65-66.

32. BWCs must be stored in a secure location with limited and controlled access (see paragraphs 60-70 and 74-80). There must be a process in place to account for BWCs daily to prevent the loss of data and to ensure that they are in good working order. Each centre must have a nominated BWC system administrator who is responsible for ensuring that all BWCs are accounted for daily, and that any footage is fully downloaded.

Using Body Worn Cameras Outside a Centre

33. Where a centre intends to deploy staff equipped with BWCs outside the centre itself, (such as during external resident escort, hospital escort, bed watch, or perimeter patrols) the use and rationale must be documented within the centre's Local Security Strategy.

34. BWCs can capture a large amount of sensitive information that may have no evidential value, but if lost or disclosed could have a negative impact on members of the public as well as reputational damage to the organisation. The activation of cameras outside a centre should be used minimally and proportionately to circumstances or incidents intended to be captured.

35. When using BWCs outside a centre, the user should be conscious they are potentially capturing data (audio and video) of members of the public who may be unaware they are being recorded. To minimise the potential for this type of collateral intrusion and

limit the potential requirement for footage to have to be pixilated or redacted by the contracted service provider, the user of the BWC should consider ceasing recording at the earliest opportunity once an incident is resolved.

36. At the point of starting to record, BWC users must ensure that they make an audible announcement that the BWC is in use and manage any objections to being filmed as soon as it is possible to do so.

37. Any objection to being filmed must be addressed by the user of the BWC with a clear and concise explanation as to why recording is taking place. The user may also explain that nonevidential material is only retained for a maximum period of 90 days and that any access to the material is both limited and controlled.

Handheld Cameras (HHCs)

38. For security and audit purposes, BWCs should be used in preference to HHCs. However, there will be certain circumstances when a HHC should be used alongside, or instead of a BWC. HHCs may provide better quality footage than BWCs during a planned relocation incident where the use of force is assessed as a possibility. In these cases, HHCs with built in memory can be used.

39. HHCs must not be used to:

    - Film covertly
    - Record general work practices
    - Record interactions between any persons without specific cause
    - Record the conduct of any type of search of a person. (See para 16 for exemptions to this)

40. If the HHC records audio, the guidance on staff identifying themselves to the camera outlined in paragraph 18 should be followed.

41. Contracted service providers must ensure that there is a process in place to account for HHCs daily, to prevent the loss of data and to ensure that they are in good working order. Once the recording has ceased, the data should be downloaded from the device at the earliest possible opportunity and within a maximum of 3 working days and stored in accordance with paragraphs 60-70.

Closed Circuit Television (CCTV)

42. Where CCTV is installed, it should only be used for official purposes and to meet the following needs:

- To prevent escape
- To detect threats to safety and security
- To detect crime
- To monitor the movement of vehicles and people through secure areas

43. Particular attention should be given to the location of these cameras to ensure that they fulfil these purposes and do not capture excessive or irrelevant personal data.

44. As a minimum, contracted service providers must undertake daily checks of their CCTV systems and records of these checks should be maintained. Any errors within the system, for example a camera not working, should be reported to the centre's security manager or other appropriate manager as soon as possible. Any **critical** failures of any CCTV system for a significant period or where a significant area under surveillance cannot be monitored, must be reported to the local Compliance Manager, or on-call manager if out of hours, and the DS Data Protection Practitioner (DPP), as soon as possible. Where the loss of CCTV occurs for either a significant period, or in a significant area of the Centre, consideration must be given for the use of alternative measures, i.e., increased staff patrols.

Escort Vehicles

45. There must be a policy in place which details the requirements and use of surveillance cameras during escorts undertaken by the escort supplier using vehicles fitted with surveillance cameras. The recording equipment within vehicles and any recorded footage should be treated in accordance with the requirements set out in this order. This policy is subject to approval by the Head of Escorting Services and must be reviewed annually by the Escorting Supplier.

46. Notices should be displayed within all escort vehicles notifying those in the vehicle that surveillance cameras are in use. The notices should also detail the process for those subject to surveillance to access material, including an escort or contracted service provider contact telephone number for the detained individuals to use in case of query or complaint.

47. For any incident involving the use of force, or the use of restraints during escort, all relevant use of force paperwork must be completed and submitted to the Home Office use of force monitor. DSO 07/2016 use of restraints for escorted moves provides further guidance on the use of restraints on detained individuals under escort.

Aerial Drones

48. Unmanned Aerial Vehicles (UAVs) or camera drones should only be used in specific circumstances. For example, where CCTV cannot be installed or there is an increased security risk in an area of a centre that would justify the use of a drone.

49. The potential risks for collateral intrusion should be considered before the decision to implement this measure is made. If risks cannot be mitigated against then a drone should not be used, and other security measures should be applied. Examples of risk mitigation include, pixelation or complete anonymisation of individuals captured on the camera, fixed field of view and limitations on the drone altitude.

50. Where drone usage is being considered by a contracted service provider for security purposes, the Home Office must be fully consulted and justification for the drone must be set out. A full DPIA must be completed, and the software and hardware must be assessed by Home Office Cyber Security/Migration & Borders Transformation Portfolio (MBTP) before implementation.

51. If a decision is made to utilise a camera drone, then it must be registered with the Civil Aviation Authority (CAA) and local police. Drone controllers must be fully trained and accredited for their operation.

52. As with CCTV, drones should only be used for official purposes and for the following requirements:

    - To prevent escape
    - To detect threats to safety and security
    - To detect crime
    - To monitor the movement of vehicles and people through secure areas

53. Appropriate signage including contact details must be clearly visible both inside and outside the centre in the areas where the drone will be mobilised in case of query or complaint.

Targeted Surveillance

54. If a surveillance camera is used to actively monitor an individual or group, whether inside or outside the IRC (for example during a protest), it should be conducted in accordance with the procedures set out in DSO 02/2015 Regulation of Investigatory Powers Act 2000 (RIPA). Once directed surveillance is considered operationally necessary, the Home Office Central Authorities Bureau (CAB) should be contacted before any activity takes place. That is unless an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable

for an authorisation under Part II of RIPA to be sought for the carrying out of the surveillance.

55. Staff should note that surveillance can only be sought for purposes related to the prevention and detection of crime or in the interests of public safety. The CAB will quality assure the surveillance application to assure its compliance with the legislation, before forwarding this to the Home Office authorising officer (i.e., the Head of Security in DSST) for authorisation.

56. If the application is submitted outside of normal office hours, the IRC security team should contact the on-call member of staff within DSST to contact the Head of Security or another RIPA Authorising Officer. RIPA (or RIPSA "Regulation of Investigatory Powers (Scotland) Act 2000") authorisation should be gained beforehand. The authorising officer, usually the Head of the CAB must give authorisations in writing, except in urgent cases when they may be given orally. An urgent case for oral authorisation should only be made if the person making the surveillance application, believes that the time required for an authorising officer to grant a written authorisation would be likely to endanger life or jeopardise the investigation for which the authorisation was being sought.

57. In such cases, contact should first be made with the CAB to confirm the case meets the urgent oral criteria. The applicant will then be put in contact with the authorising officer to discuss the case. Both the applicant and authorising officer should make contemporaneous notes of their conversation and record the date and time the authorisation was given. Urgent oral authorities last 72 hours from the time the surveillance was first authorised, unless renewed.

58. All stages of a surveillance application submitted to the CAB should be done through the automated system.

59. RIPA/RIPSA provides a framework to ensure investigatory techniques are used in a way that is compatible with the Article 8 right to respect for private and family life, enshrined in the European Convention on Human Rights (ECHR). RIPA/RIPSA ensures that these techniques are used in a regulated way and provides safeguards against the abuse of such methods. Use of these covert techniques will only be authorised if considered legal, necessary, and proportionate.

Storage and retention of footage

60. Under the DPA 2018, those operating surveillance camera systems or those who use, or process images and information obtained by such systems, must have a clearly defined retention policy to control how images and information are stored and who has access to them.

61. Irrespective of any potential criminal procedures, the inappropriate access, deletion, or alteration of any records obtained from surveillance camera systems for which the Home Office is the Data Controller, constitutes a breach of security and may lead to the suspension or revocation of the Home Office certification of custodial staff, or disciplinary action against Home Office staff.

62. All stored surveillance camera footage must be classified as Official-Sensitive under government security classifications. Stored camera footage and all communications containing such footage must contain the following handling instructions:

    OFFICIAL SENSITIVE - Contains personal sensitive information, subject to confidentiality requirements under the Data Protection Act 2018. Do not circulate this information further without prior approval from [insert details of local Information Security Manager].

63. Surveillance camera footage should, where possible, be stored on encrypted memory cards or hard drives and held in a locked cupboard. Access to this area must be restricted to reduce the risk of data loss and/or unauthorised access to footage.

64. A record should be kept as an audit trail of how images and information are handled including details on who accessed them (for example police, contracted service provider, Home Office), when and why. Access to footage should be restricted and no footage must be viewed without a justifiable reason, which must be documented within the audit trail. This audit trail must be available to the local Detention Services Compliance manager (grade HEO or above) on request and will be subject to ad hoc reviews by the Home Office.

65. Data should be stored using an agreed reference number and must not include the details of individuals on the footage within the file name. The names of the subjects on the footage should be held separately and should include the reference number of the footage.

66. If surveillance camera footage is not stored on encrypted removable media and locked in a secure location, BWC/HHC material must be uploaded onto the data processor's IT system as soon as practically possible, to ensure that the data is securely saved. Once uploaded, the contracted service provider duty manager must decide if the footage is either non-evidential or evidential (likely to be required at a future point as evidence such as use of force) and then mark the material accordingly. This marking should include the time, date, and a reference number.

67. Evidential footage may include footage of events before and after an incident. It may also include the recording of events where an incident hasn't occurred, for example, the preparatory actions of a planned relocation of a detained individual, where use of force is assessed as a possibility.

68. All non-evidential surveillance camera footage must be retained for a minimum of 120 days. This retention period is important because there may be occasions that a detained individual, staff member, or visitor makes a complaint about an incident and retaining the footage for this length of time, the period in which a complaint can be made as set out in DSO 03/2015 - handling of complaints, will ensure that it is available to view in these circumstances. If a complaint is made, any relevant footage previously classed as non-evidential must be retained in line with evidential footage retention periods (see paragraph 69). The same steps should be followed for footage where the contracted service provider is made aware of legal challenges to which the footage may be relevant. Non-evidential footage should be securely destroyed, usually by being over-written, after 120 days to comply with UK data protection law.

69. All evidential footage (i.e., use of force, assault, or any other serious incident) must be retained for a minimum of 6 years to ensure it is available in case of litigation. If footage has been marked as 'evidential footage', it must be transferred to an encrypted memory stick or hard drive and stored in a locked cupboard with access restricted.

70. At least once a month, the contracted service provider security manager must review 5% of the month's recordings to ensure that the use of the camera was justified, the quality of the recording is sufficient and that it is being retained and tagged appropriately. Any footage that raises concerns or records an incident that had not been previously identified, must be escalated, and addressed appropriately. Auditable records of these checks must be maintained and be available to the Compliance Team on request.

Deleting footage

71. If the footage has been transferred onto an encrypted portable/plug-in memory card, cloud storage or hard drive, this should then be deleted from the IT system. Once this memory card or hard drive has passed its retention date and is no longer needed, the footage should be deleted, so that the memory card or hard drive can be re-used. (Where internal hard drives are utilised e.g., in recording units, these should be destroyed in the first instance).

72. The contracted service provider must ensure that when footage is deleted, it is removed from any computer systems in its entirety. It is recommended that the software used for deletion of footage complies with HMG infosec standard No.5[8].

73. An audit trail should be available for all historical footage demonstrating the history of the data from filming to storage, subsequent access, and deletion. This record should be made available to the Compliance Team on request.

[8] https://www.ncsc.gov.uk/guidance/information-risk-management-gpg-47

Access to footage

74. A system operator should have clear polices and guidelines in place to deal with any requests for access to footage that are received. A data audit trail recording what footage has been reviewed, by whom and the reasons why, must be kept for every occasion footage is accessed. This should include when the footage has been reviewed for the purposes of quality control. The audit trail should be made available to Home Office managers on request. Decisions about the disclosure of material should be made by the Home Office (as Data Controller) who has the discretion to refuse any request for information unless there is an overriding legal obligation, such as a court order or information access rights, with input from the contracted service provider (as data processor). In case of query, the contracted service provider should approach their local Home Office Immigration Enforcement Delivery Manager for advice.

75. All footage must be made available to the Home Office within 24 hours of a request. Centre Managers, or any senior manager given the authority to do so, may access surveillance camera material where there is a clear and justifiable need to do so.

76. Footage may also be requested by internal departments, such as the Independent Examiner of Complaints or other organisations / departments, for example other government departments and agencies; local authorities; police and other law enforcement agencies, courts, and other judicial bodies, His Majesty's Inspectorate of Prisons (HMIP) or the Prison and Probation Ombudsman (PPO) (note that the PPO has unfettered access to BWC footage). These requests should be sent to the data processor via email, including the reason for the request, and should be responded to within 48 hours. If access is granted, the data (including accompanying audio and any necessary redactions), should be made available within an additional 72 hours. The Home Office should be notified of all such requests and, where material is provided this should be done using some form of portable media which is either encrypted / password protected or via a secure HO approved online sharing platform, such as 'MOVEit'. This should be via a signed chain of custody, such as secure internal Home Office dispatch pouches or via recorded delivery.

77. If a detained individual requests a copy of the data that is being held about them, they must apply in writing, to the Home Office via the Personal Information Charter on the Home Office page of GOV.UK (Personal Information Charter), or by submitting a Subject Access Request (SAR). On receipt, the Home Office team will discuss the request with the Delivery Manager and contracted service provider. If the Home Office is obliged to answer the request, the contracted service provider (as the data processor) must provide the information to the Home Office as soon as possible, and at the latest within 30 days, to ensure that the Home Office is able to respond to the request within the 40-day time limit as set out in the Data Protection Act 2018.

78. If a contracted service provider or the Home Office receives a subject access request (SAR) or a legal request to disclose surveillance images of individuals or of an incident, the footage must be reviewed by the contracted service provider to establish whether the identifying features of any of the other individuals in the image (whether detained individuals or staff) or secure areas shown in the footage, as well as security features such as locks or keys, need to be obscured. If disclosed, the contracted service provider, in conjunction with the Home Office, is responsible for ensuring that any third-party images are obscured, whether undertaken in-house by the contracted service provider or by an external organisation which meets all current data protection standards.

79. If the SAR (Subject Access Requests) team or Government Legal Department (GLD) agree it is appropriate to disclose the footage (including accompanying audio and any necessary redactions), arrangements should be agreed with the SAR team or GLD (as relevant) as to how it should be viewed: either on-site or by disclosing footage in a redacted format. If onsite, the contracted service provider is responsible for planning with the requestor/legal representatives to view the footage in a secure setting at the IRC. If the footage is to be redacted for disclosure, the costs of paying for the footage should be split dependant on the origin of the request i.e., for Home Office Litigation, costs will be covered by the Home Office. For internal matters, the contracted service provider would cover any costs associated with redaction of footage. Where CCTV is to be redacted (only when it is needed for an investigation, litigation, or alternative organisation that receives the SAR e.g., PPO), the contracted service provider must cover any costs associated with redaction of CCTV. These types of requests are often time-sensitive and therefore, each supplier should have a process in place agreed by the Home Office Delivery Manager, ready for when a request is received. All requests for access to data must be formally recorded by the contracted service provider for audit purposes.

80. Healthcare staff must not use BWC/HHCs. The use of CCTV in healthcare areas in England should only be undertaken with the authority of NHS England who is the Data Controller in these circumstances., Information on the relevant NHS England contact for data access should be displayed in the centre and a local policy must be in place for their use. As outlined in paragraph 16, surveillance cameras should not be used in healthcare facilities (excluding waiting rooms), unless there are exceptional circumstances (e.g., first responders to a serious incident) and their use is strictly necessary to gather evidence, and there is no other reasonable means of gathering the necessary evidence.

Training

81. All contracted service provider staff who use surveillance cameras or manage surveillance camera data, should have a good understanding of the legislation

controlling its use and be trained on the operation of the equipment. This training should also include:

- The circumstances in which BWC/HHCs can be used (see paragraphs 17 and 27)
- Diversity issues and the provisions of ECHR
- When to commence and cease recording
- The importance of identifying recordings for retention or deletion

82. Local policy and procedures should be included in initial training courses for all staff and should be updated on an annual basis which should include regular reviews to develop practice.

Revision History

Review date	Reviewed by	Review outcome	Next review
Feb 2018	Frances Hardy	General update	Feb 2020
May 2024	Anitha Sundaram	Updated to reflect: • The roll out of Home office teams and responsibilities. • Changes to the details of which each local policy on the use of surveillance camera systems must include. • The use of annex A, relative to the use of force paperwork. • The use of surveillance camera systems in waiting rooms of healthcare facilities. • Details regarding SV1(Security Vetting) application forms, and the use of BWCs (Body Worn Camera) outside a centre. • Addition of Aerial Drones	May 2026
August 2025	Jessica Hayson	• Removal of “prayer rooms” from list of areas not to have cameras installed.	May 2026