Ministry of Justice

HM Prison & Probation Service

Use of CCTV (Overt Closed-Circuit Television system) Prison Guidance

CONTENTS

Guidance

This document is for Prison use only and offers further guidance on the use of CCTV for surveillance purposes within the Prison Service.

1. Current CCTV legislation

The Prison Rules 1999
https://www.legislation.gov.uk/uksi/1999/728/contents/made

The Prison (Amendment) (No. 2) Rules 2000
https://www.legislation.gov.uk/uksi/2000/2641/article/6/made

The Young Offender Institution Rules 2000
https://www.legislation.gov.uk/uksi/2000/3371/contents/made

Data Protection Act 2018 (DPA) and UK General Data Protection Regulation (UK GDPR)
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Protection of Freedoms Act 2012
https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

Freedom of Information Act 2000
https://www.legislation.gov.uk/ukpga/2000/36/contentsSurveillance Camera Code of Practice published by the Home Office
https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

2. Code of Practice

Please see the below link for the Information Commissioner's Office Code of Practice:

https://ico.org.uk/for-organisations/guide-to-data-protection-1998/encryption/scenarios/cctv/

3. ICO guidance

3.1 What is CCTV used for?

CCTV is used to maintain the safety and security of Her Majesty's Prison and Probation Service (HMPPS) by monitoring the activity of individuals within the estate. It should be made clear to data subjects (the identified or identifiable living individual to whom personal data relates) that they are under surveillance by the use of CCTV and that a recording is taking place.

CCTV is used to prevent and detect crime, and maintain the security, safety, training and good management (including adjudications) of HMPPS. HMPPS should ensure that prisoners/children, visitors and employees are given notice and made aware of the purpose of the monitoring. This should be communicated clearly on signage; further detail on

signage can be found in section 3.3. CCTV must not be used for the sole purpose of monitoring staff performance.

Establishments should keep a record of CCTV footage which has been downloaded for any purpose. The log should include all details of downloaded footage, including when footage has been disclosed or retained. An example of a CCTV Evidence Log is included in Annex A; the example includes but is not limited to;

- Log number
- Evidence details
- Name of subject/s
- Type of incident
- Location of incident
- Reason for retention beyond 30 days
- Continuity details
- Has this been disclosed; why and to who?
- Reason for retention beyond 3 months (relevant to information held under Prison Rule 50A) and date of review

Use of CCTV for Training Purposes

If there is a requirement to use CCTV surveillance for training purposes, consideration should be given to alternative methods which would serve the purpose, other than using CCTV footage. HMPPS could suffer reputational damage whenever personal information is being used or shared incorrectly. If no alternative is viable or appropriate, then CCTV footage can be used and the requirements in the policy framework would apply to its use. But this must be considered on a case by case basis. The following are points of consideration:

- Is anyone in the footage identifiable (also from anyone's knowledge of the incident)?
- What is the setting of the incident recorded and is it contentious?
- Is the footage being used informally in a debrief setting, or is the footage going to be used as part of a larger/more formal training event?

If you have considered the above and these cannot be met, using this footage for training purposes could be high risk in terms of data protection, and you should complete a Data Protection Impact Assessment (DPIA) to consider the risk and determine if the use is justifiable. Information on DPIAs can be found via the below link:

https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/privacy-reform/data-protection-impact-assessments-dpias/

For more information on individual cases, please refer to the Information Security and Services Team (FMB). Please see Annex B for a quick reference guide on using CCTV for training purposes.

3.2 Where the CCTV is sited

Both permanent and movable cameras must be placed in such a way to ensure that the only images captured are of areas that are the subject of surveillance; for example, an individuals' private property should not be the subject of surveillance.

CCTV should not be sited in places where there is a heightened expectation of privacy, such as shower or toilet facilities, and in clinical suites in healthcare.

3.3 Responsibilities – signage

People must be made aware they are in an area where a surveillance system is in operation and the reason why it is being used.

The most effective way of doing this is by using prominently placed signs at the entrance to the surveillance system's zone and reinforcing this with further signs inside the area. Clear and prominent signs are particularly important where the surveillance systems are very discreet, or in locations where people might not expect to be under surveillance. Generally, signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a surveillance system.

Prison industries provide CCTV signs for HMPPS for a cost and can be contacted directly for procurement purposes. This will be a "soft charge only" so should be utilised above other procurement routes. See Annex C.

<u>Complaints</u>

More information on prisoner/child complaints and the use of CCTV is detailed in the Prisoner Complaints Policy Framework, which can be found via the below link:

https://intranet.noms.gsi.gov.uk/policies-and-subjects/policy-frameworks/prisoner-complaints-policy-framework

For staff, they are advised to follow their local internal complaints procedure but can also refer a complaint to the ICO if they believe there has been a breach of their rights under the UK GDPR and the DPA.

Visitors can raise a complaint to the Prison Service if they believe there has been a breach of privacy and can also refer any complaint to the ICO.

Information on how to make a complaint is also detailed in the relevant privacy notice, which are available upon request.

3.4 Viewing

Viewing of live images on monitors is restricted to the Operator and any other permitted person (as determined by the Governing Governor) where it is necessary for them to see it and is limited to those who are required to be able to view footage as part of their duties. Recorded images should also be viewed in a restricted area in the prison, such as a designated secure office. Details of permitted personnel should be clearly defined in the

establishments Local Security Strategy (LSS). Recorded images which have been sent to partner agencies for evidential or investigative purposes can be viewed outside of the prison.

Playback of CCTV coverage is only permitted in the following circumstances:

- Where it is suspected that security has been compromised
- The prevention and detection of crime
- Safety
- To assist an investigation / good management of the prison for safeguarding the security, good order and discipline of the establishment (including an adjudication and referrals to the Police)
- Response to immediate events; i.e. hostage situation, concerted indiscipline, activation of alarm bells etc.
- Training purposes to ensure all of the above

Encrypted digital transfer should be used (where available) for the downloading of evidence, however discs and flash drives are permissible with authorisation. Evidence should be shared digitally to partner agencies where possible; where this is not possible, a secure courier service should be used.

For further information about the use of CCTV in the Adjudication process, please refer to PSI 05/2018 Prisoner Discipline Procedures (Adjudications).

Good practice would be to keep a record of who has been authorised to view retained footage; an example of an authorisation form for this purpose is detailed in Annex D.

3.5 Disclosure of Information (including Subject Access Requests and Freedom of Information Requests)

Disclosure of information from surveillance systems must be controlled and consistent with the purpose for which the system was established. Any disclosure of CCTV footage must be documented, and a record kept (e.g Annex A).

HMPPS have discretion to refuse any request for information unless there is an overriding legal obligation, such as a court order or information access rights. Once you have disclosed information to another body, such as the Police, they become the data controller for the copy they hold. It is their responsibility to comply with the DPA/UK GDPR in relation to any further disclosures, and this should be communicated clearly to any organisation who information is disclosed to. The method of disclosing information should be secure to ensure that it is only seen by the intended recipient.
Requests for information should be approached with care as wider disclosure may be unfair to any third parties captured in the footage. When disclosing surveillance images of individuals consideration must be given as to whether the identifying features of any third parties in the images needs to be pixelated.

Where CCTV footage of a visit has been obtained, any footage obtained can only be disclosed where all parties to the visit consent to its disclosure. However, if there is a lawful basis for disclosing the footage any identifying features of third parties (unconnected to the

data subject(s)) captured during the visit will be pixilated removing the requirement for consent.

The Pixilation Team assist with obscuring/pixilating images, and can be contacted on the below email address:

PixilationTeam@justice.gov.uk

Please refer to the ICO Code of Practice for further information regarding disclosure and encryption:

https://ico.org.uk/for-organisations/guide-to-data-protection-1998/encryption/scenarios/cctv/

For the requirements relating to the disclosure of CCTV footage obtained under Prison Rule 50A, please see the requirements section and paragraph 4.4 of the policy framework.

Subject Access Requests

You may receive requests from individuals for information you hold on them, such as CCTV footage. Individuals whose information is recorded have a right to be provided with that information or, if they consent to it, view that information. These requests are likely to be received from prisoners and children in custody, ex-offenders, children and visitors to the prison or staff.

Freedom of Information (FOI) Requests

You may also receive requests for information under the Freedom of Information Act 2000 (FOIA) relating to the use of surveillance systems. For example, requestors may ask for information regarding the operation of the systems, the siting of them, or the costs of using and maintaining them. If this information is held, then consideration will need to be given to disclosure under FOIA. The implied presumption within FOIA is towards disclosure, unless an appropriate exemption applies.

For further information, or if a Freedom of Information or Subject Access Request (SAR) is requested (from someone who is not a prisoner, ex-offender or young person, e.g. staff, prison worker or visitor), please contact the Disclosure Team who will be able to advise you. SARs from prisoners, ex-offenders or young persons for their prison and/or probation files should be sent to the Offender Subject Access Request Team who will be able to advise you further.

Disclosure Team: data.access@justice.gov.uk
Offender Subject Access Request Team: data.access1@justice.gov.uk

Death in Custody investigations

Following a death in custody (or any other investigation) relevant CCTV footage may be requested by the Prisons and Probation Ombudsman (PPO) and the Coroner to assist them in their independent investigations into the death. The PPO has unfettered access to CCTV footage, and it must be disclosed to the PPO when requested as part of any investigation. It should also be noted that when footage following a fatal incident is retained, it must include

all relevant footage (including that from the landing outside of a cell) as it is important to see earlier interactions leading up to the discovery. This includes, but is not limited to:

- All CCTV footage from the last time the person entered the cell and up to and including the discovery of the death.
- If the person was subject to ACCT monitoring, as a minimum, all CCTV footage from outside of the cell covering the 48 hours leading up to the death.

Advice on disclosure in these circumstances can be sought from the Safer Custody Casework team and Government Legal Department.

3.6 Disposal of Information

Where it is not necessary to retain information, for example, it does not achieve the purpose for which you are collecting and retaining information, then it should be deleted, and the deletion recorded (e.g. Annex A). For more information on retention please see section 7.2.

4. Privacy Notice

HMPPS is part of the Ministry of Justice (MoJ). The MoJ is the data controller for the personal information we hold in HMPPS.

Privacy notices explain the standards that can be expected from HMPPS:

- when HMPPS request, obtain, use or hold personal information;
- how to access a copy of your personal data;
- how to complain if policy has not been followed.

Privacy notices can be found on the intranet for prisoners, prison visitors, staff and the Youth Custody Service (YCS). A paper version of these should also be available upon request.

Please see the link below to access the privacy notices for prisoners, prison visitors and the YCS. The privacy notice for staff is included as an Annex E.

https://intranet.noms.gsi.gov.uk/support/InfoSec/gdpr

5. UK General Data Protection Regulation (UK GDPR) Requirements

The essential purpose of UK GDPR is to safeguard personal data; balancing the legitimate needs of organisations to obtain and use personal data with the rights of individuals to privacy. The law set out the requirements that organisations, such as HMPPS, need to adhere to when processing personal information. It also stipulates a number of rights for individuals in relation to how their personal data is processed and managed.

CCTV recordings, as information held by HMPPS, are subject to the UK GDPR and the DPA 2018 and must be handled in compliance with that legislation.

6. Alternative options to CCTV within HMPPS

If it is not appropriate to use CCTV, there are several procedural solutions which could be more suitable for maintaining and monitoring the security of the estate, these include:

- Patrolling of the perimeter
- The use of patrol and search prison dogs (See PSI 2011/20 Prison Dogs)
- Searching of the person (See PSI 2016/07 and PSI 2012/08)
- Searching of cells, bedrooms, areas and vehicles (See PSI 2016/09 and PSI 2012/08)
- Use of Body Worn Video Cameras (See PSI 2017/04 NSF: Body worn video cameras)

7. Storage and Retention of CCTV footage

7.1 Storage of Information

Recorded material should be stored in a way that maintains the integrity of the information. This is to ensure that the rights of individuals recorded by surveillance systems are protected and the information can be used effectively for its intended purpose.

The way in which information should be held and recorded, ensuring that access is restricted, should be carefully considered. Information should be secure and encrypted where necessary.

If material is downloaded or recorded for evidential purposes, an audit trail of this process should be captured. Once material is burned off or recorded, it becomes physical evidence, and should be dealt with accordingly. Please refer to Prison Service Instruction 2016/08 Dealing with Evidence for further information.

7.2 Retention

The DPA does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage, however for HMPPS it is advised that all information is not retained beyond 30 calendar days. This may vary depending on the purpose of the recording and can be determined on a case by case basis.

If information is to be held longer than 30 days, the retention period should be informed by the purpose for which the information is collected and how long it is needed to achieve this purpose. It should not be kept for longer than is necessary and should be the shortest period necessary to serve the purpose.

This should not be determined simply by the storage capacity of a system. Where it is not necessary to retain information, for example, if it does not achieve the purpose for which it is collected and retained, then it should be deleted.

There will be circumstances where you may need to retain information for a longer period. For example, where a law enforcement body investigates a crime and request for it to be preserved, to provide them opportunity to view the information, as part of an active investigation (such as an adjudication), or for litigation purposes. Please refer to PSO 1300

Investigations, PSI 06/2010 Conduct and Discipline, and as detailed in section 6.7.1, please refer to PSI 2016/08 Dealing with Evidence.

Information should not be downloaded generally unless it is for evidential purposes, however there may be exceptional circumstances. If information is burned off or downloaded for any reason other than for evidential purposes, this will need to be authorised by the Governing Governor. Guidance retention periods for litigation purposes are listed below.

- CCTV footage relating to personal injuries should be retained for 3 years 4 months, in line with limitation periods for personal injury claims.

- Footage of all prisoner on prisoner assaults (child on child), even low-level injuries, should be retained for 3 years 4 months, unless Control & Restraint was used where it should be retained for 6 years.

- CCTV footage relating to Use of Force incidents should be kept for 6 years.

- CCTV footage relating to a death in custody should be kept for 6 years.

Footage may be required by the PPO, and an establishment should not decide what footage is relevant. If an incident takes place within a cell and there is no footage of in-cell events, footage captured on the landing before, during and after the alleged incident should not be routinely deleted.

Where an accident, complaint or local investigation mentions CCTV footage, a copy of this footage must be retained. The establishment should decide locally who is responsible for this. Copies must be retained onsite physically or electronically (where available) when providing copies to external colleagues, such as the Police, the Independent Monitoring Board (IMB), the Prison and Probation Ombudsman (PPO) etc. More information on the PPO can be found in PSI 58/2010 The Prison and Probation Ombudsman.

Footage should be stored electronically where available to avoid loss or damage and to reduce the need for resources to store physical evidence. An electronic log could also be kept to ensure footage is stored for the correct length of time and destroyed when appropriate.

Litigation teams should be provided with copies of footage electronically where available, either by uploading footage to the Health and Safety data collection portal or providing the team with direct access.

The retention of CCTV footage obtained during a visit or under Prison Rule 50A/YOI Rule 54 due to constant supervision of prisoners and children is handled separately. The retention of any footage must be in accordance with specific Prison Rules and shall not be retained for longer than 3 months, unless its continued retention is necessary on grounds specified in Rule 35A(4) and proportionate to what is sought to be achieved by the continued retention of the footage. Where footage is retained for longer than 3 months, it's continued retention must be reviewed every 3 months. If following a review its continued retention is no longer necessary, the Governor must arrange for the footage to be destroyed. Further information is detailed in the requirements.

Please see Annex F for a quick reference guide on the retention of CCTV footage.

8. Locations in HMPPS of note

8.1 Accommodation

Constant Supervision

The use of CCTV for someone on Constant Supervision significantly limits the possibility of meaningful engagement and the amount of information you are able to understand about the person receiving support. It therefore must not be used routinely to replace face to face contact, and face to face constant supervision should always be the default option unless constant supervision of a prisoner/child is necessary and proportionate under Rule 50A of the Prison Rules 1999 (YOI Rule 54). For more details see the policy framework.

When deciding if CCTV can be used, consideration must be given as to how this would impact staff's ability to intervene in an emergency, as staff need to be able to intervene immediately.

As mentioned in section 4.18, it must be made clear to the person requiring support that CCTV is being used and the use of CCTV must also be recorded within the Assessment Care in Custody Teamwork (ACCT) document (ongoing record and Case Review notes). Where CCTV is used to monitor a prisoner/child on Constant Supervision, this must be monitored by staff at all times so that staff are able to intervene immediately in the event of an emergency. Attempts to actively engage with the person must still be made to reduce risk. This includes regular face-to-face check-ins and attempts to engage them in meaningful conversation and distraction activities.

8.2 Chaplaincy

The use of CCTV is permitted in places of worship only for security and safety purposes. Video recording is allowed where prison chaplains have private conversations with prisoners/children but audio recording for intelligence gathering purposes (for which authorisation is required) cannot be used.

8.3 Mother and Baby Units (MBU)

The use of CCTV is permitted in MBU but is not mandated. Establishments may wish to consider the specific benefits of CCTV in communal areas within MBU, in relation to the safeguarding responsibilities for children residing on them. CCTV must not be used in areas of an MBU where privacy is required; this includes areas in which women feed or wash their babies.

8.4 Other areas

This Policy Framework also applies to movable cameras which are overtly deployed to support the CCTV network (e.g. not as part of a targeted intelligence led deployment), including motion activated cameras. Prior to movable cameras being used, any deployment

must be authorised. The process for authorising this must be documented, an example of this is detailed in Annex G; this example includes but is not limited to;

- Purpose of deployment including evidence of need
- Requested by
- Authorised by
- Any risks and mitigation
- Start date of deployment
- Review date (must be every 3 months as a minimum)
- End date of deployment

Any ongoing movable camera deployment must be reviewed every three months as a minimum. It is also good practice to keep a record of when movable cameras have been deployed; an example log of this is detailed in Annex H.

The decision to deploy devices must be authorised by the Head of Security or Deputy Governor and can be recorded in the minutes of the monthly security meeting as best practice. This is to ensure the decision to deploy movable cameras can be challenged appropriately and ensure that consideration of whether a Directed Surveillance Authority should be sought is made.

Wherever possible, to mitigate against potential data loss either due to theft of the device, loss/damage of the device for causes unknown, such devices should not use removable media storage. Advice on appropriate devices can be sought from the Technical Surveillance Unit if required.