CCTV Policy

## Audience:

1. This policy compliments the Ministry of Justice’s overall security policy.
2. This CCTV Policy applies to all employees, contractors, partners and service providers, including those on co-located sites and sites owned by other public bodies. This will also include employees of other organisations who are based in, or work at, Ministry of Justice occupied premises.
3. Agencies and arm’s length bodies (ALBs) are expected to comply with this corporate framework but may establish their own arrangements tailored to operational needs and should supplement it with local policy/guidance for any business-specific risk.

## Objective:

1. The MoJ has in place several CCTV surveillance systems installed within its core buildings. This policy details the purpose, usage and management of the CCTV systems, and the procedures to be followed to ensure the MoJ complies with relevant legislation and the current Information Commissioner’s Office (ICO) Code of Practice.
2. The MoJ have due regard to the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), the Freedom of Information Act 2000, the Protection of Freedoms Act 2012 and the Human Rights Act 1998. The MoJ also has due regard to the Surveillance Camera Code of Practice, issued under the Protection of Freedoms Act 2012 and the 12 guiding principles contained therein.
3. This policy is based upon guidance issued by the Information Commissioner’s Office (ICO).
4. This policy and the procedures detailed, applies to the MoJ CCTV systems including security guards’ body worn cameras. CCTV images are monitored and recorded in strict accordance with this policy.
5. This policy is applicable to all buildings owned or occupied by the MoJ where MoJ monitored CCTV is installed.

## Scope and Definition:

1. The CCTV systems are owned by the MoJ, managed by the MoJ Group Security Team and its appointed security sub-contractors. Under the Data Protection Act 1998 and the UK General Data Protection Regulation the MoJ is the ‘data controller’ for the images produced by the CCTV system. The MoJ system is registered with the ICO. The CCTV system operates to meet the requirements of the Data Protection Act and the Information Commissioner’s Guidance.
2. The Chief Security Officer is responsible for the overall management and operation of the CCTV systems, including activities relating to installations, recording, reviewing, monitoring and ensuring compliance with this policy.
3. The CCTV system operates across MoJ core buildings.
4. Clearly visible and readable signs of an appropriate size are placed at all pedestrian and vehicular entrances to inform persons entering that CCTV is in operation. The signage indicates that the system is managed by the MoJ and a 24-hour contact number for the site is provided.
5. The Chief Security Officer is responsible for ensuring that adequate signage is erected in compliance with the ICO CCTV Code of Practice.
6. Cameras are sited to support the physical posture of the building, which can include all internal communal areas such as reception, stairwells and lift lobbies, perimeter areas, including car parks and walkways.
7. When siting CCTV cameras, MoJ will have due consideration for overlooking residential property.
8. The CCTV systems are operational and are capable of being monitored up to 24 hours a day, 365 days per year. This policy supports MoJ in preserving the physical security of its buildings, staff and assets and will be reviewed on a regular basis.
9. Any proposed new CCTV installation is subject to a Data Protection Impact Assessment (DPIA).

## Context:

1. The principal purposes of the CCTV systems are as follows: for the prevention, reduction, detection and investigation of crime and other incidents; to ensure the safety of our assets, which includes staff and other persons entering the buildings; to assist in the investigation of suspected breaches of MoJ HR or security policies. Privacy notices to include references to CCTV will be displayed as appropriate.
2. The CCTV system will be used to observe MoJ buildings and areas under surveillance to identify incidents requiring a response. Any response should be proportionate to the incident being witnessed.
3. The MoJ seeks to operate its CCTV system in a manner that is consistent with respect for the individual’s privacy.
4. Cameras are monitored from secured local control rooms or equivalent within our buildings which are staffed 24 hours a day. Access to control rooms are restricted to authorised staff only. Visitors to the local control rooms must always be escorted.
5. Images are stored locally within the buildings on dedicated CCTV network servers. The servers are located within secure areas to prevent unauthorised access. The cameras are viewable by authorised security staff. For urgent operational reasons, the security manager or the Facilities Manager can authorise view only access to CCTV footage. Additional staff may be authorised by the Chief Security Officer to monitor cameras sited within their own areas of responsibility on a view only basis.
6. The cameras provide images that are of suitable quality for the specified purposes for which they are installed, and the cameras are checked by the appropriate facilities management contractor to ensure that the images remain fit for purpose. They must report systems faults immediately via the appropriate maintenance contract and ensure that a log is maintained.
7. All images recorded by the CCTV system remain the property and copyright of the MoJ.
8. The monitoring of cameras will be carried out in accordance with the systems purpose.

**Responsibilities:**

1. All employees, contractors, partners, service providers and employees of other organisations who are on Ministry of Justice premises and co-located sites remain accountable for the security, health and safety of themselves, colleagues and the protection of departmental assets.

**Policy Statements:**

1. In its administration of its CCTV system, the MoJ complies with the Data Protection Act 1998. Due regard is given to the data protection principles embodied in the Data Protection Act 1998 and the General Data Protection Regulation (GDPR). These principles require that personal data shall be:
   1. processed fairly and lawfully;
   2. held only for specified purposes and not used or disclosed in any way incompatible with those purposes;
   3. adequate, relevant and not excessive;
   4. accurate and kept up to date;
   5. be kept no longer than necessary for the particular purpose;
   6. processed in accordance with the rights of individuals;
   7. kept secure; and
   8. not to be transferred outside the European Economic Area unless the recipient country ensures an adequate level of protection. For information contact [Data Privacy Team](mailto:Privacy@justice.gov.uk).
2. Comply with the UK General Data Protection Regulation. Due regard will be given to the data protection principles contained within Article 5 of the GDPR which provides that personal data shall be:
   1. processed lawfully, fairly and in a transparent manner;
   2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
   3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
   4. accurate and, where necessary, kept up to date;
   5. kept in a form which permits identification of the data subjects for no longer that is necessary for the purposes for which the personal data are processed;
   6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

*New Installations:*

1. Using surveillance systems can be privacy intrusive. They can place large numbers of law-abiding people under surveillance and recording their movements as they go about their day-to-day activities. The MoJ must consider the nature of the problem we seek to address; whether a surveillance system would be justified and an effective solution; whether better solutions exist; what effect its use may have on individuals; and whether considering this, its use is a proportionate response to the problem. Where the MoJ is already using a surveillance system, to comply with the DPO Code of Practice it will re-evaluate and record every 12 months whether it is necessary and proportionate to continue using it.
2. These matters will be considered objectively as part of the scheme’s impact on people’s privacy. This should be done by conducting a [Data Protection Impact Assessment (DPIA)](https://intranet.justice.gov.uk/guidance/knowledge-information/protecting-information/privacy-reform/data-protection-impact-assessments-dpias/).

**Applications for disclosure of images:**

*Applications by individual data subjects*

1. Requests by individual data subjects for images relating to themselves, a Subject Access Request should be submitted in writing on the request form at Annex A to [MoJ Group Security](mailto:mojgroupsecurity@justice.gov.uk), together with proof of identification.
2. In order to locate images on MoJ systems, sufficient detail must be provided by the data subject to allow the relevant images to be located and the data subject to be identified.
3. Where the MoJ is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided expressed consent to the disclosure, or if it is considered reasonable by the Chief Security Officer, having regard to the circumstances e.g. in relation to the prevention or detection or in other circumstances where an exemption applies under relevant legislation, to comply without the consent of the individual.

*Access to and disclosure of images to third parties*

1. A request for images made by a third party should be made in writing on the request form at Annex A to [MoJ Group Security](mailto:mojgroupsecurity@justice.gov.uk).
2. In limited circumstances it may be appropriate to disclose images to a third person, such as when a disclosure is required by law, in relation to the prevention of crime or in other circumstances where an exemption applies under relevant legislation.
3. Such disclosure will be made at the discretion of the Chief Security Officer, with reference to relevant legislation.
4. Where a suspicion of misconduct arises and at the formal request of the Investigating Officer or HR Manager/Advisor, the Chief Security Officer may approve viewing access to CCTV images for use in staff disciplinary cases.
5. In exceptional cases, the Chief Security Officer may approve access to copies of CCTV images to Investigating Officers when sought as evidence in relation to discipline cases.
6. A record of any disclosure made under this policy will be held securely by MoJ Group Security on the access record at Annex B itemising: the date, time, camera, requestor, authoriser and the reason for disclosure.

**Retention of Images**

1. Unless required for evidential purposes, the investigation of an offence or as required by law, CCTV images will be retained for no longer than 31 days from the date of recording after which images will be automatically overwritten.
2. Where an image is required to be held in excess of the retention period following an application for disclosure of images, the Chief Security Officer or their nominated deputy, will be responsible for authorising such as request.
3. Images held in excess of their retention period will be reviewed on a three-monthly basis and any not required for evidential purposes will be deleted.
4. Access to retained CCTV images is restricted to the Chief Security Officer and other persons as required and authorised by the Chief Security Officer.

**Complaints Procedure**

1. Complaints concerning the MoJ use of its CCTV or the disclosure of CCTV images should be made in writing to the [Physical Security Manager](mailto:MoJGroupSecurity@justice.gov.uk).
2. All appeals against the Physical Security Manager should be made in writing to the Chief Security Officer.

**Monitoring Compliance**

1. All staff involved in the operation of the CCTV System will be made aware of this policy and will only be authorised to use the CCTV System in a way that is consistent with the purposes and procedures contained therein.
2. All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake data protection training.

**Usage of CCTV**

1. The MoJ usage of CCTV and the content of this document shall be reviewed annually by the Chief Security Officer with reference to the relevant legislation or guidance in effect at the time.

## Compliance:

1. The level of risk and potential impact to MoJ assets and most importantly physical harm to our people and the public will determine the controls to be applied and the degree of assurance required. MoJ must ensure a baseline of physical security measures are in place at each site and receive annual assurance that such measures are in place to provide appropriate protection to all occupants and assets, and that these measures can be strengthened when required i.e. in response to a security incident or change in the Government Response Level.
2. The implementation of all security measures must be able to provide evidence that the selection was been made in accordance with the appropriate information security standards ISO27001/27002, Physical Security advice taken from the Centre for the Protection of National Infrastructure and [Government Functional Standard GovS 007: Security](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903904/Government_Security_Standard.pdf) (link is external).
3. The constantly changing security landscape has necessarily dictated that Physical Security measures be constantly re-evaluated and tested in order to meet new threats and other emerging vulnerabilities. This policy and subsequent supporting standards will be subject to annual review or more frequently if warranted.

**Physical security advice:**

1. Physical security advice can be obtained by contacting MoJ Group Security: [mojgroupsecurity@justice.gov.uk](mailto:mojgroupsecurity@justice.gov.uk).

**Annexes:**

Annex A: Subject Access Request (SAR)

Annex B: Record of CCTV Disclosure – Ministry of Justice

**CCTV Subject Access Request Form**

**Please complete this complete this form to request Security Data (Subject Access Request), which is controlled by MoJ Group Security Team.**

All requests for the release of data shall be channelled through the data controller or via the nominated representatives. This request is processed accordance to the General Data Protection Regulation 2016 (GDPR). Please send this request form to: [mojgroupsecurity@justice.gov.uk](mailto:mojgroupsecurity@justice.gov.uk).

**Requesters details\*** (You must provide proof of identity)

|  |  |  |  |
| --- | --- | --- | --- |
| Name: | | | |
|  | | | |
| Organisation | | | |
|  | | | |
| Address and contact number: | | | |
|  | | | |
| Reason for request: | | | |
|  | | | |
| Please give full details of the material you are requesting to include date, time and location: | | | |
|  | | | |
| Are you requesting footage on behalf of another person/organisation (If yes, please provide details below)? | | Yes | No |
|  | | | |
| Address and contact number: | | | |
|  | | | |
| Signature | Date: | | |
|  |  | | |

For MoJ Group Security Use:

|  |  |  |  |
| --- | --- | --- | --- |
| Proof of ID: | | Yes | No |
| Type of photographic ID provided: |  | | |
| Expiry date: |  | | |
| Reference number: |  | | |

For Chief Security Officer use only:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Request to share/release CCTV footage: | | Yes | If approved, please indicate what information can be released: | | | View only | |
| No | Copy of contents | |
| Is the site required to retain a copy of the CCTV footage supplied? | | | | | | Yes | No |
| Signature: |  | | | Date: |  | | |

Site security team – Log this request and its outcome on you site CCTV Disclosure Record.

**CCTV footage must always remain secure. Access is for authorised personnel only. Copies of CCTV footage must not be retained for longer than is necessary for legal/disciplinary purposes. Retention should be reviewed with Chief Security Officer every 3-months and the outcome recorded.**

**Record of CCTV Disclosure – Ministry of Justice**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Organisation/Department** | **Details of disclosure required** | **Date of authority to release footage** | **Issued by and Date** | **Additional copy held by the MoJ (Yes/No)** | **Reviewed** | **Destroyed by** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Guidance**

When requesting CCTV disclosure, the requestor should provide full details of the information they require, including camera location and number, date and time of the footage required and the reason they require the footage.

Authority to release footage may only be provided by the Chief Security Officer (CSO) or If delegation the Deputy Security Adviser (DSA). If considered necessary for departmental security, a copy may be held by the MoJ at the discretion of the CSO/DSA. Additional copies must not be made without this authority.

The officer issuing the disclosure must identify themselves and note the date the disclosure was made.

Authority to destroy the data must be given by the CSO/DSA, who will advise a route for secure destruction