

INFORMATION SECURITY POLICY:

## CCTV Policy

Owner: Head of FM

Status: Approved

Approved by: Nolan Smith

Role: SIRO

Date: 23 February 2021

Next review date: February 2022

Version: 2.0

Classification: OFFICIAL

Version History: Minor Amendments

 2.0 Updated with Dominions House sound recording

1. Updated to OfS and incorporating good practice from the ICO

# Contents

[1. Introduction 4](#_Toc80367950)

[Purpose of the CCTV policy 4](#_Toc80367951)

[Scope of the policy 4](#_Toc80367952)

[Ownership and operation of CCTV schemes 4](#_Toc80367953)

[Principles 4](#_Toc80367954)

[2. Purpose of using CCTV 5](#_Toc80367955)

[3. Authorised staff 5](#_Toc80367956)

[Chief Executive 6](#_Toc80367957)

[Senior Information Risk Owner (SIRO) 6](#_Toc80367958)

[Head of Governance 6](#_Toc80367959)

[Data Protection Officer (DPO) 6](#_Toc80367960)

[Facilities and estates management 7](#_Toc80367961)

[IT Security Officer 7](#_Toc80367962)

[Exceptional circumstances 7](#_Toc80367963)

[4. Procedure 8](#_Toc80367964)

[Targeted observations and monitoring 8](#_Toc80367965)

[Viewing of CCTV images 9](#_Toc80367966)

[Retention of CCTV images 9](#_Toc80367967)

[5. Disclosure of CCTV images 10](#_Toc80367968)

[Subject access requests under Data Protection legislation 11](#_Toc80367969)

[Disclosure of images to third parties 11](#_Toc80367970)

[Appendix A: Surveillance Camera Code of Practice – guiding principles (Home Office, June 2013) 12](#_Toc80367972)

[Appendix B: Data protection principles 13](#_Toc80367973)

[Appendix C: CCTV scheme signage 14](#_Toc80367974)

[Appendix D: Example confidentiality undertaking 15](#_Toc80367975)

[Confidentiality agreement – disclosure of CCTV images 15](#_Toc80367976)

OfS CCTV policy

# 1. Introduction

## Purpose of the CCTV policy

The purpose of the CCTV policy is to ensure:

1. That the use of CCTV adheres to the principles of Data Protection Legislation (2018), General Data Protection Regulations (2016), Human Rights Act (1998), Regulation of Investigatory Powers Act (2000), and other relevant legislation;
2. That the use of CCTV reflects guidance from the Surveillance Commissioner (issued under the Protection of Freedoms Act) and the Information Commissioner’s Office;
3. That CCTV is fit for purpose, correctly and appropriately installed, and operated;
4. That we reduce reputational risks by staying within the law and avoiding regulatory action and penalties;
5. That we re-assure those whose information is being captured by our CCTV system that our systems and processes are legal, fair and appropriately applied.

## Scope of the policy

The policy applies to all employees and to tenants and visitors to our premises in Bristol. Responsibility for the external and reception area CCTV system at our London Office, Finlaison House, is with the Government Actuary’s Department, with whom we have an agreement for use of the building.

All CCTV installations and the operating of these systems should comply with this policy.

The CCTV policy should be read in conjunction with the Physical Security Policy.

## Ownership and operation of CCTV schemes

All cameras, monitors, data collection and retention processes will be maintained operationally by named staff. Systems are maintained by a third-party provider under separate maintenance contract to the OfS in accordance with this policy.

## Principles

The following principles will govern the operation of the CCTV system:

* The system will be operated fairly and lawfully and only for the defined purposes set out in section 2;
* The system will be operated with due regard for the privacy of individuals at all times;
* Any change to the purposes for which the system is operated will require the prior approval of the Senior Information Risk Officer having sought advice from data protection specialists as required.

# 2. Purpose of using CCTV

The primary purpose of the CCTV system is to protect our premises from criminal activities and to help reduce the fear of crime for staff, tenants and visitors (including for those who are entering and leaving the building out of normal office hours or during the hours of darkness).

The purposes of the system, unless specifically identified as targeted monitoring, are in accordance with the following:

1. To deter and reduce the incidence of crime on our premises so maintaining the security of individuals and property;
2. To reduce the likelihood of harm to our employees, contractors and visitors;
3. That, where the use of CCTV systems can make a contribution, we can meet our responsibilities under health and safety and related legislation;
4. To afford greater protection to sensitive areas that contain a large concentration of information, or because the equipment held in those areas is valuable or because tampering with the equipment could affect day to day operations, e.g. areas where server or network equipment are housed;
5. To assist us in our response to incidents arising;
6. To prevent and detect crime and facilitate the apprehension and prosecution of offenders;
7. To reduce incidences of vandalism and criminal damage to property.

# 3. Authorised staff

The following roles are authorised to view images: Head of Governance, DPO, Facilities and Estates Manager, and Operations Manager. All staff viewing images should respect the confidentiality of what they have seen and only use the information obtained for the purposes for which they were viewed.

Only the Chief Executive, SIRO, DPO, or Head of Governance may authorise the release of images. In all cases their authorised deputy may also take the decision under the scheme of delegation.

## Chief Executive

The Chief Executive (CE) (as Accounting Officer) has overall accountability for how we utilise CCTV systems including the approval, organisation and management of all CCTV systems on the premises. Approval of information security related policies, including this policy, has been delegated to the Senior Information Risk Owner. The CE has the authority to view CCTV images in exceptional circumstances only (see below), specific to carrying out their Accounting Officer responsibilities or deputising for the SIRO if unavailable. The CE has authority to permit CCTV to be used covertly and/or in working areas and/or anywhere on our premises and authorise any other person to view CCTV images in circumstances they judge to be exceptional. The CE has the authority to disclose images to any person, including third parties, as described below.

## Senior Information Risk Owner (SIRO)

The SIRO has overall responsibility for approving this policy on behalf of the Accounting Officer, which should ensure that the CCTV policy meets our legal and other obligations, and adequately mitigates the risks relevant to the use of CCTV. In circumstances they judge to be exceptional, the SIRO has the authority to:

1. View CCTV images, specific to carrying out their SIRO responsibilities or deputising for absent staff who have authority;
2. Authorise any other person to view CCTV images;
3. Permit CCTV to be used covertly, and/or in working areas and/or anywhere on our premises only when the CE is unavailable to make this decision;
4. Disclose images to any person, including third parties, as described below.

## Head of Governance

The Head of Governance will have responsibility for approving the disclosure of images and is authorised to view and report on relevant CCTV images for this purpose. In the absence of the Head of Governance, the Data Protection Officer has the authority to undertake this role except where, in the DPO’s view, it conflicts with their statutory role. This includes ensuring that, when images are subject to review, the relevant staff are made aware of the data privacy/protection aspects of the use of CCTV systems and any ongoing obligations of confidentiality.

## Data Protection Officer (DPO)

The DPO may view the images insofar as they need to in order to be able to provide advice in the context of their obligations under data protection legislation. The DPO may also exercise the responsibility of the Head of Governance, as described above, when the Head of Governance is unavailable.

## Facilities and estates management

The Facilities and Estates Manager is responsible for the oversight and management of the CCTV system, which incorporates ensuring that systems and procedures are in place to ensure compliance with this policy.

## IT Security Officer

The IT Security Officer (or IT staff authorised by the IT Security Officer) may provide technical assistance in the operation of the system, e.g. in copying and/or storing images authorised for disclosure and supporting the secure disclosure of them to a third party. While the IT Security Officer (or IT staff working on their behalf) are not ordinarily authorised to view images, it is accepted that assisting with the operation of the CCTV system may necessitate viewing of images. If a cyber incident has occurred, the ITSO may, if appropriate, request authorisation to view images to check for unauthorised devices, such as USB sticks being inserted. During security audits the ITSO may also request assurance the CCTV is working and is compliant with retention policies by checking the system configuration is correct.

## Exceptional circumstances

Almost by definition, the meaning of exceptional circumstances for the purposes of this policy cannot be fixed as they will be dependent on the circumstances of the situation. However, they include a need to alleviate, or mitigate, unforeseen or unconventional circumstances, including the personal circumstances of any individual. They should be consistent with the purposes of using a CCTV system as described above.

Exceptional situations and incidents are relatively unusual and likely to happen only infrequently. The CE and SIRO are in responsible roles and are considered able to make judgements to this effect. Advice should normally be taken from the Head of HR (or HR Consultant) if there are risks to an individual(s) in making such a decision.

Exceptional circumstances include where covert filming may be authorised, e.g. to help prevent physical injury or prevention of crime. This will only take place when it has been authorised in writing by the Chief Executive and limited to a specific period of time and, as far as possible, to specific people or a specific location.

Filming in areas where staff would reasonably expect privacy (toilets, changing rooms, and the medical room) will not normally be authorised unless there are the most exceptional circumstances arising, e.g. a request by the police, and that this would require the specific written authority of the Chief Executive, who must take advice from the Head of HR and the DPO.

We will emphasise that in all cases the risk of intrusion on innocent employees will be balanced against the objectives of the covert filming as part of the authorisation process.

# 4. Procedure

The Facilities Management team will maintain and operate procedures intended to implement this policy. These procedures will ensure the CCTV system will be operated in accordance within the guidelines issued by the ICO and the Surveillance Commissioner.

1. Suitable operation, backup, retention, destruction and maintenance of all storage media will be conducted taking account of Home Office and British Security Industry Association operational standards;
2. Cameras will not be hidden from view. CCTV will not normally be used to record activity in working areas, but CCTV may be used in these areas in exceptional circumstances, with the permission of the CE or SIRO;
3. There is no sound recording undertaken from Nicholson House and Westward House System but Dominions House cameras are equipped with this facility;
4. Signs to inform staff, visitors to the premises and the public of the presence of a CCTV system and its ownership will be displayed at all times (see Appendix C for guidance on signage);
5. To ensure privacy, all CCTV cameras will only be focussed on our property;
6. Viewing monitors will be sited so that all recorded images can only be viewed by authorised staff;
7. Images from the cameras are appropriately recorded in accordance with operational procedures maintained by the Head of Facilities Management.

## Targeted observations and monitoring

CCTV will not normally be used to record activity in working areas or to target specific activity or individuals, but CCTV may be used in these ways where the CE or SIRO judge the circumstances to be exceptional. The reasons for doing so must be recorded in every case and they should only be in accordance with the declared purposes or objectives and notification of the monitoring should be provided to the Data Protection Officer. The Head of Governance and Head of Facilities Management are permitted to authorise the use of CCTV for these purposes when the circumstances require an urgent decision and the CE and SIRO are unavailable within the relevant timescale. Wherever possible the advice of the Data Protection Officer should be sought in these circumstances.

The Regulation of Investigatory Powers Act 2000 regulates the use of targeted surveillance of this type. Use for any other reason other than that authorised in accordance with this policy is not permissible at any time.

Use of CCTV in a targeted way will be authorised only for a specified period and if this needs to be extended, fresh authorisation will be necessary before the expiration of the specified period.

## Viewing of CCTV images

Viewing of CCTV images will be restricted to those members of staff who need to have access to the system in order to achieve the purpose for which the system has been installed; “the authorised staff”.

The authorised staff are shown above.

Authorised staff can view images for the purposes stated without seeking further authority. A record will be kept each time the system is formally viewed stating who viewed the images, when they were viewed and the reason for doing so. This record will be retained to facilitate the audit of usage should it be required. Any sensitive or personal details in the log or record should be kept for no longer than six months from the date it was recorded, although this may subsequently be anonymised and retained for up to three years to facilitate an understanding of the use of the CCTV system over time.

Authorised staff must ensure that they comply with this policy and any associated procedures.

## Retention of CCTV images

Access to the system containing retained images is restricted to the Head of Facilities Management, the Deputy Head of Facilities Management and the IT Security Officer (or someone working under the direction of the IT Security Officer). Other staff authorised to view images only have access to the system to view images when they have cause to do so.

For the purposes described in section 2 above, CCTV images will ordinarily be kept for no longer than one month, but with a reserved right to keep images for a maximum of three months within the core CCTV system. Copies of images taken in response to incidents may be retained for up to six months. Either time limit may be extended subject to the approval of the Head of Governance, DPO or SIRO as described below. These time limits are intended to balance the business need with the rights of individuals. In more detail:

1. The CCTV system records images when a sensor detects movement. Therefore, the recorded images are retained for as long as there is space in the memory of the recording system, rather than for a specific time. In line with recognised practice and police advice, we will normally hold images for not longer than four weeks. However, because there is a risk the activity captured is minimal (e.g. because of low periods of activity or cameras failing to operate), we reserve the right to hold routine images for up to three months. Any extensions to this time limit require the approval of the Head of Governance, DPO or SIRO.
2. Specific CCTV images may be copied and held in a secure location for a longer period where an incident requiring attention requires access to the images. In such cases, the images will normally be held for no longer than 6 months; this may be extended only where there is a clear and ongoing process, e.g. a court case requiring access to the images may take longer than six months and, where a claim against us is possible, the claimant has three years in which to do so. Any such extensions require the approval of the DPIM, DPO or SIRO.

# 5. Disclosure of CCTV images

The disclosure of CCTV images means allowing someone else (beyond those authorised above to view them) to view images and/or to be provided with a copy of images, whether they are a member of staff or a third party). Disclosure must be consistent with one or more of the purposes stated above, or where permitted or required to do so by law or (where justifiable) to assist a third party to comply with the law.

All the OfS officers listed above are able to view images and have the authority to approve the disclosure of images to third parties following consultation with one other listed officer. However, in the case of the group two listed officers (Facilities and Estate Manager and the Facilities Operations Manager) consultation must be with a member of group one.

Only the Facilities and Estate Manager, the IT Security Officer (or IT staff authorised by the IT Security Officer) may take a copy of the images to provide to a third party once this has been authorised. The method of disclosure should be secure, e.g. secure encrypted email.

In considering the disclosure of CCTV images, judgement may need to be made where images contain information on individuals not involved in the incident concerned. In most cases, the privacy intrusion to such individuals will be minimal and obscuring images need not be required (see also DPA item below). In such cases, consideration should be given to the nature and context of the CCTV footage. In some limited circumstances, it may be appropriate to disclose information to a third party, where their needs outweigh those of the individual whose information is recorded. The rationale for such decisions should be recorded in writing.

## Subject access requests under Data Protection legislation

Data Protection legislation gives individuals the right to access personal information about themselves, including CCTV images, by making a Data Subject Access Request (DSAR).

Individuals are entitled to be provided with a copy in a permanent form of all the information caught by the request that constitutes their personal data unless an exemption applies. We may offer data subjects the opportunity to view the CCTV images on our premises. As this constitutes ‘disclosure’, authorisation must be sought for this as described above, noting that a DPA request will normally be overseen by the Head of Governance. If so, data subjects are permitted to bring a colleague or PCS representative (if employed by us) to view the CCTV images with them, provided all those viewing the images are made aware of the data privacy/protection aspects of the use of CCTV systems. A confidentiality agreement may be used if the officer authorising the viewing judges it necessary.

Where third party data is visible, we will consider whether it is technically possible or practicable for this information to be obscured. Third parties may be approached to seek their agreement to allowing their personal information to be viewed.

All requests for access to CCTV images should be made in writing.

## Disclosure of images to third parties

Disclosure of CCTV images to a third party may constitute viewing and/or providing a copy of images to the third party. Either or both is permissible subject to the following:

1. Subject to situations where viewing of CCTV images is assessed by the authorising officer as both necessary and urgent, all requests by a third party to see the images must be made in writing (this can be by email). The request must be accompanied by a clear explanation of the purpose of the request, how the images will be used and when, and under what circumstances, they will be destroyed. Where urgent requests are fulfilled, details of the request with accompanying information should be recorded in writing within two working days of the disclosure.
2. Disclosure of images must be controlled to protect the rights of the individual and ensure that a chain of evidence remains intact. A confidentiality agreement to be signed by the person to whom images are provided may be used if the officer authorising the viewing judges it necessary. An example confidentiality agreement is provided at Appendix D. This may be adapted for use or, alternatively, a bespoke agreement may be prepared if this version is unsuitable for the circumstances arising.
3. CCTV images must not be disclosed, to individuals or third parties, without first seeking the approval of the Head of Governance or, if they are unavailable, having sought the advice of the Data Protection Officer (DPO) which must be received in writing. This requirement may be waived for urgent cases if the Head of Governance (or DPO) are unavailable, or the advice may be provided orally, to be followed up and provided in writing within two working days.
4. The copying and transfer of images to a third party must be undertaken using secure means.
5. Summarising the request in a log of requests by third parties for CCTV footage. This will record the date and time of the disclosure along with details of who the information has been provided to and why they required it. This information will be retained for at least as long as the images are retained

Third parties may include, for example, the police, our employees, contractors, insurance companies working on behalf of staff, visitors, and members of the public.

# Appendix A: Surveillance Camera Code of Practice – guiding principles (Home Office, June 2013)

|  |  |
| --- | --- |
| 1 | Use of a surveillance camera must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need. |
| 2 | The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified. |
| 3 | There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints. |
| 4 | There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used. |
| 5 | Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them. |
| 6 | No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged. |
| 7 | Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes. |
| 8 | Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards. |
| 9 | Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use. |
| 10 | There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published. |
| 11 | When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value. |
| 12 | Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date. |

# Appendix B: Data protection principles

**Under the GDPR, the data protection principles set out the main responsibilities for organisations.**

Article 5 of the GDPR requires that personal data shall be:

“a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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.”

Article 5(2) requires that:

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

# Appendix C: CCTV scheme signage

The Data Protection Act 2018 states that we have a duty to let people know that they are in an area where CCTV cameras operate, and that signs should:

* Be of appropriate size, clearly visible and readable (at least A5 size)
* Provide details of the organisation operating the system
* State the purpose for using CCTV and who to contact about the scheme.

It is particularly important to place signs in areas monitored by CCTV where people might not expect to be under surveillance.

# Appendix D: Example confidentiality undertaking

*To be used/adapted as appropriate to the circumstances where such an agreement is considered necessary by the officer authorising the release of CCTV images.*

## Confidentiality agreement – disclosure of CCTV images

### Background

The Office for Students (OfS) has agreed to provide a copy of some CCTV images it holds to XXX on (date). These comprise (add brief description of the nature of the images e.g. suspicious behaviour in the car park arising on (date/time). The images to be disclosed run for X minutes/seconds.

### Conditions of the undertaking

In being provided with CCTV images belonging to the OfS, XXX agrees that these images contain (or may contain) personal sensitive information as defined in data protection law and therefore must be processed accordingly, including where it contains images of people unrelated to the request to see the images.

XXX’s reasons for seeking this information are (describe reasons provided by requestor).

Through this undertaking, XXX agrees they will:

1. Only use the images provided for the purpose(s) stated.
2. Restrict access to these images within your own organisation to only those people who have a need to see them in accordance with the agreed purpose(s).
3. Not divulge or communicate these images to any third party in the UK or elsewhere, other than where this explicitly relates to the purpose(s).
4. Become the data controller for the images in accordance with the extant data protection legislation.
5. Comply with relevant Home Office guidance or any other relevant legislation.
6. Destroy the CCTV images when they have been used for the agreed purpose or when requested to do so by the OfS, whichever is earlier.

Signed:

……………………………………………………… Date ……………………………………

(Insert name)

Authorising officer for and on behalf of: (insert name of company etc., if needed)