Registers of Scotland

Security and Information Assurance

Registers of Scotland
Departmental Security Group
Policies and Procedures

Department	Security and Information Assurance (SIA)			
Topic	Security – CCTV Policy			
Number	SIA 19			
Amended	**By**	SIA	**Date**	29 August 2016

THE USE OF CLOSED CIRCUIT TELEVISION (CCTV) TO COMPLY WITH THE DATA PROTECTION ACT 1998

1 About this Policy

This Policy provides guidance and good practice advice for RoS staff, or contractors operating on RoS's behalf, involved in operating CCTV and other devices which view or record images of individuals. It also covers other information derived from those images that relates to individuals (for example vehicle registration marks).

This Policy uses the terms 'CCTV' and 'images' throughout for ease of reference. Information held by RoS that is about individuals is covered by the Data Protection Act 1998 (DPA) and the guidance in this Policy will help us comply with our legal obligations under the DPA.

The DPA not only creates obligations for RoS, it also gives individuals rights, such as the right to gain access to our details and to claim compensation when they suffer damage. The basic legal requirement is to comply with the DPA itself. This Policy follows the Information Commissioner's recommendations on how the legal requirements of the DPA can be met.

The procedures in this Policy are all based on the legally enforceable data protection principles (Appendix 1) that lie at the heart of the DPA and they have been set out to follow the lifecycle and practical operation of CCTV. Each section of the Policy answers the questions that must be positively addressed to help ensure that good practice is being achieved.

The procedures in this Policy will:

1.1 Ensure that those capturing images of individuals comply with the DPA;

1.2 Mean that the images that are captured are usable; and

1.3 Reassure those whose images are being captured.

Data Protection Act 1998:

CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act. This Policy is associated with the RoS Data Protection Policy, the provisions of which should be adhered to at all times.

2 What this Policy covers

This Policy covers the use of CCTV and other systems which capture images of identifiable individuals or information relating to individuals for any of the following purposes:

2.1.1 Seeing what an individual is doing e.g. monitoring them in accessing RoS' property.

2.1.2 Potentially taking some action in relation to an individual; e.g. handing the images over to the police to investigate a crime.

2.1.3 Using the images of an individual in some way that will affect our privacy; e.g. passing images on to a TV company.

Our CCTV is directed at viewing and/or recording the activities of individuals. This means that most uses of CCTV by us will be covered by the Data Protection Act (DPA) and the provisions set out in this Policy.

Appendix 2 is for situations where CCTV may be used to monitor our own staff.

Note: The DPA applies to images captured by CCTV therefore this Policy does not cover the use of dummy or non-operational cameras if employed.

2.2 The system

2.2.1 The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; Public information signs.

2.2.2 Cameras will be located at strategic points on RoS property, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view.

2.2.3 Signs will be prominently placed at strategic points and at entrance and exit points of RoS property to inform staff, visitors and members of the public that a CCTV installation is in use.

2.2.4 Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

2.3 Purpose of the system

2.3.1 The system has been installed by RoS with the primary purpose of reducing the threat of crime generally, protecting RoS's property and helping to ensure the safety of RoS's staff and visitors consistent with respect for the individuals' privacy.

These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff and assist in providing evidence to managers and/or to a member of staff against whom disciplinary or other action is, or is threatened to be taken.

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

2.4 Selecting and siting the cameras

Any CCTV images must be adequate for the purpose for which they are being collecting. It is essential that camera equipment and locations are chosen which achieve the purposes for which we are using CCTV.

Both permanent and movable cameras will be sited and image capture restricted to ensure that they do not view areas that are not of interest and are not intended to be the subject of surveillance, such as individuals' private property.

The cameras must be sited and the system must have the necessary technical specification to ensure that images are of the appropriate quality.

Siting criteria include;

2.4.1 Carefully chose the camera location to minimise viewing spaces that are not of relevance to the purposes for which we are using CCTV.

2.4.2 Consideration will be given to setting the system up so it only records at the time when the problem usually occurs

2.4.3 Have other privacy-friendly ways of processing images been considered such as only recording events that are likely to cause concern, such as movement into a defined area.

2.4.4 Site the cameras to ensure that they can produce images of the right quality, taking into account technical capabilities and the environment in which they are placed.

2.4.5 Ensure the location is suitable, bearing in mind the light levels and the size of the area to be viewed by each camera.

2.4.6 Site the cameras so that they are secure and protected from vandalism.

2.4.7 Ensure the system produce images of sufficient size, resolution and frames per second.

2.4.8 To judge the quality of images that will be necessary, the purpose for which CCTV is used and the level of quality that will be necessary to achieve the purpose must be considered. This can be achieved under the following four categories;

2.4.9 Monitoring: to watch the flow of traffic or the movement of people where we do not need to pick out individual figures.

2.4.10 Detecting: to detect the presence of a person in the image, without needing to see our face.

2.4.11 Recognising: to recognise somebody we know, or determine that somebody is not known to RoS.

2.4.12 Identifying: to record high quality facial images; which can be used in court to prove someone's identity beyond reasonable doubt.

3 Using the equipment

CCTV systems must produce images that are of a suitable quality for the purpose for which the system was installed. Poor quality images will undermine the purpose for installing the system.

3.1 Ensure the recorded pictures and prints as well as the live screens produce good clear pictures. Check that there has not been an unacceptable loss of detail during the recording process.

3.2 Considered the compression settings for recording material in a digital system, a high level of compression will result in poorer picture quality on playback.

3.3 Set up the recording medium in such a way that images cannot be inadvertently corrupted.

3.4 Regularly check that the date and time stamp recorded on the images is accurate

3.5 Set up a regular maintenance regime to ensure that the system continues to produce high quality images.

3.6 If a wireless transmission system is used, ensure sufficient safeguards are in place to protect it from being intercepted.

CCTV must never be used to record conversations between members of the public; systems without this facility will be chosen if possible. If the system comes equipped with a sound recording facility then this will be turned off or disabled. Limited circumstances in which audio recording may be justified include:

3.7 Audio based alert systems (such as those triggered by changes in noise patterns such as sudden shouting). Conversations must not be recorded.

3.8 Two-way audio feeds from 'help points' covered by CCTV cameras, where these are activated by the person requiring assistance.

3.9 Conversations between staff and particular individuals; where a reliable record is needed of what was said.

3.10 Where recording is triggered due to a specific threat, e.g. a 'panic button' in a taxi cab.

In these circumstances, signs must make it very clear that audio recording is being or may be carried out.

The use of audio to broadcast messages to those under surveillance will be restricted to messages directly related to the purpose for which the system was established.

3.11 Ensure audio monitoring or recording capability has this been disabled

3.12 If an audio based alert system is being used put in place measures to prevent conversations being monitored or recorded.

3.13 If there are audio communications with help points, are these initiated by those requiring assistance?

3.14 If a message broadcast facility is used, are the messages limited to those consistent with the original purpose for establishing the system?

4 Recorded material and using the images

4.1 Storing and viewing the images

Recorded material will be stored in a way that maintains the integrity of the image. This will protect the rights of individuals recorded by the CCTV system and ensure that the material can be used as evidence in court. We will keep a record of how the images are handled as they may be used as evidence in court. Once there is no reason to retain the recorded images, they will be deleted. When we delete the images will depend on the purpose for using CCTV.

It is important that our images can be used by appropriate law enforcement agencies if this is envisaged. If they cannot, it will undermine the purpose for undertaking CCTV surveillance.

4.1.1 It will be easy to take copies of a recording off our system when asked for by a law enforcement agency

4.1.2 This will be done without interrupting the operation of the system

4.1.3 They will find our recorded images straightforward to use?

4.1.4 Procedures are in place for when recorded material needs to be taken away for examination

Viewing of live images on monitors will be restricted to the operator. Recorded images are viewed in a restricted area. The monitoring or viewing of images from areas where an individual would have an expectation of privacy will be restricted to authorised persons.

4.1.5 Our monitors are correctly sited taking into account the images that are displayed

4.1.6 Our monitor viewing area is appropriate and secure

4.1.7 Access is limited to authorised people

4.2 Disclosure

Disclosure of images from the CCTV system is controlled and consistent with the purpose for which the system was established. Images may be released to the media for identification purposes; this will only be done by a law enforcement agency.

Any other requests for images will denied, as a wide disclosure of these may be unfair to the individuals concerned.

In some limited circumstances it may be appropriate to release images to a third party, where our needs outweigh those of the individuals whose images are recorded. Prior to disclosure consideration will be given to;

4.2.1 Whether the request is genuine

4.2.2 Any risk to the safety of other people involved.

4.2.3 Ensuring arrangements are in place to restrict disclosure of images in a way consistent with the purpose for establishing the system

4.2.4 Clear guidance is available on the circumstances in which it is appropriate to make a disclosure and when it is not

4.2.5 Recording the date of the disclosure along with details of who the images have been provided to (the name of the person and the organisation they represent) and why they are required.

We 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 we have disclosed an image to another body, such as the police, then they become the data controller for our copy of that image. It is our responsibility to comply with the Data Protection Act (DPA) in relation to any further disclosures. The method of disclosing images is secure to ensure they are only seen by the intended recipient.

4.3 Retention

Retention periods are reflections of the purposes for recording images. We will not keep images for longer than necessary to meet our purposes for recording them. All images are digitally recorded and stored securely within the systems hard drive, for up to 30 days when they are then automatically erased.
On occasion, we may need to retain images for a longer period, where a law enforcement body is investigating a crime, to give them opportunity to view the images as part of an active investigation.

4.3.1 We will decide the shortest period that we need to retain the images, based upon our own purpose for recording the images

4.3.2 Our image retention policy is documented and understood by those who operate the system.

4.3.3 Measures are in place to ensure the permanent deletion of images through secure methods at the end of this period.

4.3.4 We undertake systematic checks to ensure that the retention period is being complied with in practice

4.4 Subject access requests

Individuals whose images are recorded have a right to view the images of themselves and to be provided with a copy of the images. This will be provided within 40 calendar days of receiving a request. We may charge a fee of up to £10 (this is the current statutory maximum set by Parliament). Those who request access must provide details which allow us to identify them as the subject of the images and also to locate the images on our system.

We will consider:

4.4.1 Staff involved in operating the CCTV system will be able to recognise a subject access request.

4.4.2 We have internal procedures in place for handling subject access requests

4.4.3 This will include keeping a log of the requests received and how they are dealt with, in case we are challenged.

4.4.4 A clearly documented process is in place to guide individuals through such requests. This makes clear what an individual needs to supply.

We will decide:

4.4.5 What details do we need to find the images

4.4.6 It is made clear whether an individual will need to supply a photograph of themselves or a description of what they are wearing at the time they believe they are caught on the system, to aid identification

4.4.7 It is made clear whether details of the date, time and location are required

4.4.8 What fee will be charged for supplying the requested images (up to a maximum of £10) and how will it be paid.

4.4.9 Make this clear to people making access requests. How will we provide an individual with copies of the images?

If images of third parties are also shown with the images of the person who has made the access request, we will consider whether we need to obscure the images of third parties. If providing these images would involve an unfair intrusion into the privacy of the third party, or cause unwarranted harm or distress, then they will be obscured. It may be necessary to contract this work out to another organisation. Where this occurs, we will need to have a written contract with the processor which specifies exactly how the information is to be used and provides us with explicit security guarantees.

4.5 Deciding to use, or continue with, CCTV

Using CCTV can be privacy intrusive, as it is capable of putting staff, contractors and members of the public under surveillance and recording our movements as we go about day to day activities. Careful consideration will be given whether to use it; the fact that it is possible, affordable or has public support will not be the primary motivating factor. The benefits to be gained will be taken into account along with whether better solutions exist and what effect it may have on individuals.

Example: Cars in a car park are frequently damaged and broken into at night. Consider whether improved lighting would reduce the problem more effectively than CCTV.

These matters will be considered objectively as part of an assessment of the CCTV's impact on people's privacy. The extent of assessment necessary will depend on the size of the proposed scheme and the level of impact it is likely to have on people's privacy[1]. The results of the impact assessment will determine whether CCTV is justified in all the circumstances and if so how it will be operated in practice.

The things covered in an impact assessment will include:

4.5.1 What the organisation will be using with the CCTV images?

4.5.2 Who will take legal responsibility under the Data Protection Act (DPA)?

4.5.3 What is the organisation's purpose for using CCTV?

4.5.4 What are the problems it is meant to address?

4.5.5 What are the benefits to be gained from its use?

4.5.6 Can CCTV technology realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?

4.5.7 Do we need images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?

4.5.8 Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?

4.5.9 What future demands may arise for wider use of images and how will we address these?

4.5.10 What are the views of those who will be under surveillance?

4.5.11 What could we do to minimise intrusion for those that may be monitored particularly if specific concerns have been expressed?

RoS may also need to consider wider human rights issues and in particular the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life). This will include:

4.5.12 Is the proposed system established on a proper legal basis and operated in accordance with the law?

4.5.13 Is it necessary to address a pressing need, such as public safety, crime prevention or national security?

4.5.14 Is it justified in the circumstances?

4.5.15 Is it proportionate to the problem that it is designed to deal with?

4.5.16 If this is not the case then it would not be appropriate to use CCTV.

5 Administration

Establishing a clear basis for the handling of any personal information is essential and the handling of images relating to individuals is no different. This policy establishes;

5.1 Responsibility for the control of the images, for example, deciding what is to be recorded,

5.2 How the images will be used and to whom they may be disclosed. The body which makes these decisions is called the data controller and is legally responsible for compliance with the Data Protection Act (DPA).

Where another organisation is involved, each will know its responsibilities and obligations. If both make decisions about the purposes and operation of the scheme, then both are responsible under the DPA. The Information Commissioner's Office (ICO) will be notified who is the data controller and the notification will cover;

5.3 The purposes for which the images are used,

5.4 The disclosures that are made and,

5.5 Other relevant details

If someone outside RoS provides us with any processing services, for example editing the images a written contract will be in place with clearly defined responsibilities. This will ensure that the images are only processed in accordance with our instructions. The contract will include guarantees about security, such as storage and the use of properly trained staff.

Clear procedures are established which determine how the system is used in practice. These procedures;

5.6 Clearly identify and define the specific purposes for the use of images, and communicate this to those who operate the system

5.7 Are clearly documented and

5.8 Have been given to appropriate people

5.9 Also, responsibility for ensuring that procedures are followed is allocated to an appropriate named individual

The named individual will ensure that

5.10 Standards are set,

5.11 Procedures are put in place to meet these standards

5.12 The system complies with this Policy and with legal obligations such as an individual’s right of access.

5.13 Proactive checks or audits carried out on a regular basis to ensure that procedures are being complied with and

5.14 Regularly review whether the use of CCTV continues to be justified.

6 Responsibilities

6.1 Letting people know

We will prominently place signs at the entrance to the CCTV zone and reinforce this with further signs inside the area. Signs will be more prominent and frequent where it would otherwise be less obvious to people that they are on CCTV. In the exceptional circumstance that audio recording is being used, this will be stated explicitly and prominently.

Signs will:

6.1.1 Be clearly visible and readable;

6.1.2 Contain details of the organisation operating the system, the purpose for using CCTV and who to contact about the scheme (where these things are not obvious to those being monitored); and

6.1.3 Be an appropriate size depending on context for example, whether they are viewed by pedestrians or car drivers.

6.1.4 We have signs in place informing people that CCTV is in operation?

6.1.5 Our signs convey the appropriate information.

Standard Text: “Images are being monitored and recorded for the purposes of crime prevention and public safety. This scheme is controlled by Registers of Scotland. For more information, call 0131 659 6111.”

6.2 Freedom of information

RoS has a member of staff who is responsible for responding to freedom of information requests, and understands the Registers responsibilities. They will respond within 20 working days from receipt of the request. Section 40 of the FOIA and section 38 of the FOISA contain a two-part exemption relating to information about individuals. If we receive a request for CCTV footage, we will consider:

6.2.1 Are the images those of the requester? If so then that information is exempt from the FOIA/FOISA. Instead this request will be treated as a data protection subject access request.

6.2.2 Are the images of other people? These will be disclosed only if disclosing the information in question does not breach the data protection principles. In practical terms, if individuals are capable of being identified from the relevant CCTV images, then it is personal information about the individual concerned. It is unlikely that this information can be disclosed in response to an FOI request as the requester could potentially use the images for any purpose and the individual concerned is unlikely to expect this. This may therefore be unfair processing in contravention of the Data Protection Act (DPA).

Note: Even where footage is exempt from FOIA/FOISA it may be lawful to provide it on a case-by-case basis without breaching the DPA, where the reason for the request is taken into account.

6.3 Other responsibilities

Staff operating the CCTV system will be aware of two further rights that individuals have under the DPA. They will recognise a request from an individual to prevent processing likely to cause substantial and unwarranted damage or distress (s10 DPA) and one to prevent automated decision-taking in relation to the individual (s12 DPA). If we receive such requests guidance will be sought from the Information Commissioner's Office. If any CCTV system covers a public space, we will be aware and comply with any licensing requirements imposed by the Security Industry Authority. Where operatives are supplied under a contract for service a public space surveillance (CCTV) licence will be in place.

7 Staying in control

Once we have established a CCTV system we will ensure that it continues to comply with the Data Protection Act (DPA) and the Policy's requirements in practice. If requested we will:

7.1 Inform people how they can make a subject access request,

7.2 Inform people who it will be sent to and what information needs to be supplied with our request;

7.3 Provide them a copy of this Policy or details of the Information Commissioner's Office (ICO) website https://ico.org.uk/about-the-ico/who-we-are/scotland-office/ and

7.4 Inform them how to complain about either the operation of the system or failure to comply with the requirements of this Information Commissioner's Code of Practise.

Staff using the CCTV system or images will be trained to ensure they comply with this Policy. In particular, they will know:

7.5 What the organisation's policies are for recording and retaining images

7.6 How to handle the images securely

7.7 What to do if they receive a request for images, for example, from the police

7.8 How to recognise a subject access request and what to do if they receive one

All images will be protected by sufficient security to ensure they do not fall into the wrong hands. This will include technical, organisational and physical security. For example:

7.9 Sufficient safeguards are in place to protect wireless transmission systems from interception

7.10 The ability to make copies of images is restricted to appropriate staff

7.11 Where copies of images are disclosed, they are safely delivered to the intended recipient

7.12 Control rooms and rooms where images are stored are secure.

7.13 Staff are trained in security procedures and there are sanctions against staff who misuse CCTV images.

7.14 Staff are aware that they could be committing a criminal offence if they misuse CCTV images.

Documented procedures which we produce following on from this Policy will be reviewed regularly, either by a designated individual within the organisation or by a third party. There is a periodic review (at least annually) of the system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, it will be stopped or modified.

A system of regular compliance reviews is in place, including compliance with the provisions of this Policy, continued operational effectiveness and whether the system continues to meet its purposes and remains justified. The results of the review recorded, and its conclusions acted upon

Appendix 1

The Data Protection Act 1998:

Data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

(a) At least one of the conditions in Schedule 2 of the Act is met, and

(b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 of the Act is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This is not a full explanation of the principles. For more general information, see The ICO's "Data Protection Act 1998 Legal Guidance" is available on the ICO website:

https://ico.org.uk/

https://ico.org.uk/about-the-ico/who-we-are/scotland-office/

Data Protection Act 1998:

Appendix 2

Monitoring our workforce

When we install CCTV in a workplace, it is likely to capture pictures of workers, even if they are not the main subject of surveillance. If the purpose of the CCTV is solely to prevent and detect crime, then we will not use it for monitoring the amount of work done or compliance with company procedures.

Have the cameras been installed so they are not directed specifically to capture images of workers?

Are the recorded images viewed only when there is suspected criminal activity, and not just for routine monitoring of workers? Cameras installed for preventing and detecting crime will not be used for non-criminal matters.

Are images of workers used only if we see something we cannot be expected to ignore, such as criminal activity, gross misconduct, or behaviour which puts others at risk?

If these images are used in disciplinary proceedings, is the footage retained so that the worker can see it and respond? A still image is unlikely to be enough.

In some cases, it may be appropriate to install CCTV specifically for workforce monitoring. We will go through the decision making process in this Policy and consider whether it is justified. In particular, consider whether better training or greater supervision would be a more appropriate solution.

Example: We suspect that our workers are stealing goods from the store room. It would be appropriate to install CCTV in this room, as it will not involve continuous or intrusive monitoring and is proportionate to the problem.

Example: We suspect that our workers are making mobile phone calls during working hours, against company policy, and we consider installing CCTV cameras on our desks to monitor them throughout the day. This would be intrusive and disproportionate. Continuous monitoring will only be used in very exceptional circumstances, for example where hazardous substances are used and failure to follow procedures would pose a serious risk to life.

Is CCTV limited to areas which workers would not expect to be private? CCTV will not be used in toilet areas or private offices.

Are workers made aware that the CCTV is for staff monitoring and how it will be used?

How are visitors informed that CCTV is in operation?

If CCTV is used to enforce internal policies, are workers fully aware of these policies and have they had sufficient training?

Do we have procedures to deal appropriately with subject access requests from workers?

Workers will normally be aware that they are being monitored, but in exceptional circumstances, covert monitoring may be used as part of a specific investigation. Covert monitoring is where video or audio recording equipment is used, and those being monitored are unaware that this is taking place. Before approving covert monitoring, we will ask ourself:

Is this an exceptional circumstance, and is there is reason to suspect criminal activity or equivalent malpractice?

Will the cameras only be used for a specific investigation, and will they be removed once the investigation is complete?

Would it prejudice the investigation to tell workers that cameras are being used?

Have we taken into account the intrusion on innocent workers?

Has the decision been taken by senior management?

Cameras and listening devices will not be installed in private areas such as toilets and private offices, except in the most exceptional circumstances where serious crime is suspected. This will only happen where there is an intention to involve the police, not where it is a purely internal disciplinary matter.

In some cases, covert cameras installed for one investigation may turn up evidence of other criminal behaviour or disciplinary offences. We will only make use of this where the offence is serious, for example, gross misconduct or misconduct putting others at risk. It would be unfair to use evidence obtained covertly for minor disciplinary matters.

In some cases, covert monitoring may be covered by the Regulation of Investigatory Powers Act 2000 or the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPA / RIPSA). We may wish to seek advice.