CCTV Surveillance

Policy Document

Policy Index No.	Policy Sponsor	Page/s	Approved by	Date
PIN007	Operations Directorate	21	The Director of Operations	28/08/13

Related policies/standards	Date
PIN 015 Covert CCTV Surveillance policy.	28/08/13
PIN 018 Irish Prison Service Information gathering policy.	28/08/13
See Section 5 for any additional documents.	

Legacy reference of policy	Date for review of policy	Date of issue/amendment
	28/08/2015	28/08/2013

IPS Policy for CCTV

Table of Contents

1. Aim of this policy

1.1 To provide a clear, consistent and best practice approach to the operation of our CCTV.

2. Purpose of this policy

2.1 To clearly describe conditions of use for CCTV systems in the IPS.

3. Scope of this policy

3.1 This policy applies to all permanent and temporary staff members, independent contractors, subcontractors or any person with CCTV responsibilities. All persons involved in the planning, supervision or operation of a CCTV scheme should be familiar with this policy.

4. Procedures for implementation

Closed circuit television is an important and essential system that is in place in and around the prison estate to assist in maintaining the good order and security of the institutions. It is of crucial importance in order to ensure confidence in the operation of CCTV systems that there is no improper use of the equipment. Any misuse of CCTV systems is likely to damage the positive perception of CCTV in the eyes of stakeholders.

This policy is designed to assist users of CCTV systems by highlighting certain legal obligations set down in the Data Protection Acts, 1988 and 2003. In order for this policy to remain relevant to the day to day activities of CCTV operation, it will be updated as practice and understanding of the laws in this area develop. Accordingly, this Code will be kept under review to ensure that it remains relevant in the context of changes in technology, and compliant with any developments in this area.

4.1 Initiation of a CCTV System

4.1.1 CCTV systems are in place in the IPS:

a) for the safety and security of staff, prisoners and visitors;

b) to assist in maintaining the good order and security of the prison estate;

c) to deter prisoners from escaping or attempting to escape;

d) to deter those having criminal intent and to help reduce the fear of crime;

e) to assist in the detection of crime, help apprehension and prosecution of offenders;

f) to provide the IPS with information relevant to the investigation of an alleged crime;

g) to aid any IPS investigation, complaint or appeal;

h) to aid any criminal investigation;

i) to give confidence to IPS staff and visitors that they are in a safe or secure environment;

j) to provide the IPS with information relating to vehicle traffic management on property under the control of the Irish Prison Service;

k) to observe the movement of all persons within the institution and at points of entry and egress, where necessary;

l) to monitor premises;

m) to recognise IPS staff, inmates and visitors for entry or exit through specific points;

n) to improve and provide information relating to health and safety matters and

o) to see what an individual inmate or visitor is doing, for example monitoring prisoner visit sessions;

4.1.2 Respect for the individual's liberty and privacy where no criminal offence has been or is being committed should be of primary consideration; accordingly, reviewing of CCTV footage will be limited to a random 20 minutes period in a shift, unless there is a specific incident to investigate. This random 20 minute review period will be chosen each morning by an IT System (CCTV Review Randomiser) and emailed to prison management at the end of each night shift. See Appendix II.

4.1.3 Only persons authorised by the Governor shall be permitted access to the control area where monitoring takes place. In this regard, the Governor will ensure that at all times entry/exit records to the control area are maintained in a visitor's journal within the prison.

4.1.4 The Governor will at all times ensure the proper and responsible operation of the CCTV system under his/her control and ensure that all persons operating or monitoring the system are appropriately trained in the system's use and understand the restrictions and legal obligations imposed upon them by the laws in this area.

4.1.5 The Governor/Chief Officer will be afforded access to CCTV images, via the Intellex System.

4.1.6 The Governor is to ensure that all uses of the system are in keeping with the eight rules of data protection[1] and in the interest of maintaining good order and security in a prison.

4.1.7 Covert surveillance.

The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance will only be permitted on a case by case basis. (See IPS Covert CCTV policy, Appendix IV).

4.1.8 A manager or designated person shall be nominated by the Governor as Data Protection Officer, who will have responsibility for ensuring the proper, efficient and orderly day-to-day operation of the CCTV system. This person will also be responsible for access requests under the Data Protection Acts, whether for CCTV images or for other personal data held on computer or manual files.

4.1.9 The Governor shall maintain an appropriate record of the system's effectiveness in consultation with prison managers and the Director of Operations. Appropriate log books will be provided.

4.2 Siting standards

4.2.1 Governors, in consultation with the Director of Operations, shall ensure that each CCTV camera is justified and proportionate for the reasons outlined in paragraph (4.1.1). The justification for the number, location and purpose shall be recorded in a register. (A copy of the Sign off form is in Appendix III) The requirement should be reviewed in light of requirements. The provision of view-only 'personal CCTV'[2] in institutions is for Governor's and Chief Officer's use only and is to be used for this purpose only.

4.2.2 Cameras shall be sited in such a way that they only monitor those spaces which are intended to be covered by the system, and will not be installed in areas where people have a reasonable expectation of privacy such as toilets, shower rooms, staff canteens, prison cells.

4.2.3 Operators must be aware that they may only use the cameras in order to achieve the purposes for which the system has been installed (see 4.1.1). Care must be taken not to use the cameras to look into any premises, be they

[1]
1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to an individual, on request

[2] This is a link from CCTVs to the Governor's PC

public houses, shops, business premises or private dwellings. This approach must likewise be taken with any demonstration of the capabilities of the cameras. It is possible to mark areas that are not to be viewed and the system will disguise or blur the area when the camera pans in that direction.

4.2.4 Operators must also be aware of the position a camera is left in after use. A camera when not in use should be placed in the most advantageous position to record any incidents occurring in a public area within its field of vision.

4.2.5 Care should be taken to ensure that no footage of private property, external to the prison/institution environs is recorded.

4.2.6 On implementation of this policy, new signs will be provided. Signs should be placed so that members of staff, inmates, visitors and other stakeholders are aware that they are entering an area which is covered by a CCTV system. These signs should be clearly visible and legible. The signs will contain the following information:

a) the identity of the person or organisation responsible for the CCTV scheme.

b) the purposes of the scheme.

c) details of who to contact regarding the scheme.

4.3 Quality of images

4.3.1 Upon installation, an initial check should be undertaken to ensure that all equipment performs properly and satisfactorily.

4.3.2 If the system records features such as the location of the camera and/or date and time reference, these must be accurate.

4.3.3 If the system includes location and date/time reference features, users must ensure that they have a documented procedure for ensuring their accuracy.

4.3.4 Cameras must be situated so to capture images relevant to the purpose.

4.3.5 When installing cameras, consideration must be given to the physical conditions in which the cameras are located.

4.3.6 Users shall assess whether it is necessary to carry out constant real time recording, or whether the activity or activities about which they are concerned occur at specific times.

4.3.7 Cameras must be properly maintained and serviced to ensure that clear images are recorded.

4.3.8 Cameras shall be protected from vandalism in order to ensure that they remain in working order.

4.3.9 A maintenance log shall be kept by the Governor.

4.3.10 If a camera is damaged, there must be clear procedures for:

a) defining the person responsible for making arrangements for ensuring that the camera is repaired.

b) ensuring that the camera is repaired within a specific time period.

c) monitoring the quality of the maintenance work.

4.4 Processing of CCTV images

4.4.1 Images to be stored in accordance with the CCTV system in each location. Images shall not be stored on computer hard drive, unless in accordance with the system in that location. If this is the case, the same retention and disposal rules apply as set out in this policy.

4.4.2 All requests from third parties to view CCTV images shall be considered by the Governor and recorded in the relevant log.

4.4.3 The Governor shall restrict access to recorded images to a designated person or persons. Viewing areas are to be within the control areas of prisons. Unauthorised persons must not be allowed to have access to that area when a viewing is taking place.

4.4.4 All requests for CCTV footage shall be sent to the Director of Operations who may arrange for same in the following circumstances:

a) the incident recorded is of a serious nature (e.g. one that may lead to criminal proceedings).

b) a formal written request from a member of An Garda Síochána (of at least the rank of Superintendant),

c) the incident recorded is proceeding to trial.

d) a request to view the tape is received from the DPP and/or the State Claims Agency.

e) that repeated playing of the incident recorded is required (i.e. to show to witnesses).

f) a copy is required in order to satisfy a subject access request.

g) so that certain areas may be sample-monitored by managers to ensure that required tasks are being carried out to agreed standards, such as checks on special observation cells, for health, safety and welfare of inmates.

4.4.5 On removing the medium on which the images have been recorded, the Operations Directorate shall ensure that they have documented:

a) the date on which the images were copied from the general system;

b) the reason why they were copied from the system;

c) any crime incident number to which the images may be relevant;

d) the location of the images;

e) the signature of the collecting official, where appropriate.

4.4.6 Upon receipt of a request for viewing, the Governor must record the following in the relevant log:

a) the date and time of the viewing.

b) the name(s) of the person(s) viewing the images. (If this includes third parties, the name of the organisation to which the third party belongs).

c) the reason for the viewing.

d) the outcome, if any, of the viewing.

4.4.7 All operators and employees with access to images shall be made aware by the Governor of the procedures which need to be followed when accessing the recorded images.

4.4.8 Disposal of Copies

a) Any and all copies of images are to be logged and returned to the Data Protection Officer in the institution after the purpose for which they have been made is complete.

b) The copies are to be destroyed or material erased and the date of the procedure recorded in the log book.

c) The log is to be actively managed to ensure that outstanding copies are accounted for, returned quickly and erased/destroyed.

4.4.9 It is the responsibility of the Governor to ensure that all operators are aware of and trained in their responsibilities under this policy. Operators must be made aware of:

a) the user's security policy e.g. procedures for access to recorded images).

b) the user's disclosure policy.

4.5 Access to and disclosure of images to third parties

4.5.1 Access to images should be restricted to staff that require access in order to achieve the purposes of using the equipment.

4.5.2 All access to the recorded images shall be documented by the Governor or a manager or designated member of staff acting on the Governor's behalf and noted in the relevant log.

4.5.3 Disclosure of the recorded images to third parties shall only be made by the Governor, in consultation with the Director of Operations, in limited and prescribed circumstances. Circumstances in which disclosure is appropriate would, for example, include:

a) a formal written request from a member of An Garda Síochána (of at least the rank of Superintendant), for disclosure of images, on the grounds that the images are likely to be of use for the investigation of a particular offence;

b) a requirement under any enactment, rule of law or court order to disclose the images;

c) if required by the Governor's legal representatives if a case/action is being taken against the governor/staff/inmate/visitor/stakeholder;

4.5.4 All requests for access for disclosure should be recorded by the Governor. If access or disclosure is denied, the reason should be documented.

4.5.5 If access to or disclosure of the images is allowed, then the following shall be documented:

a) the date and time at which access was allowed or the date on which disclosure was made;

b) the identification of any third party who was allowed access or to whom disclosure was made;

c) the reason for allowing access or disclosure;

d) the extent of the information to which access was allowed or which was disclosed;

e) the identity of the officer authorising such access.

4.5.6 If access and disclosure of images is required, the Governor should ensure all third parties whose images are not required for the purpose stated, should be obscured by pixilation or other acceptable distortion/editing techniques. This section does not negate the requirement to identify witnesses to any event.

4.5.7 If the system does not have the facilities to carry out that type of editing, an editing company may be hired to carry out this work.

4.5.8 If an editing company is hired, then the manager or designated member of staff must ensure that:

a) there is a contractual relationship between the Governor/Irish Prison Service and the editing company;

b) that the editing company has given appropriate guarantees regarding the security measures they take in relation to the images;

c) the Governor/Irish Prison Service shall have in place appropriate and adequate procedures to ensure those guarantees are met including a right of access to the contractor's premises or systems;

d) the written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the Governor or a manager or designated member of staff acting on the Governor's behalf;

e) The written contract makes the security guarantees provided by the editing company explicit.

4.6 Access by Data Subjects[3]

Data Subject Access Standards

4.6.1 The Governor shall assign a person with responsibility for data protection matters in the institution. This person must be able to recognise a request by data subjects for access to personal data in the form of recorded images. This person will usually be responsible for CCTV matters (see Section 4.1.8)

[3] **Data Protection Acts 1998 & 2003**

5. Restriction of right of access.

5.-. (1) Section 4 of this Act does not apply to personal data- .

(c) in any case in which the application of that section would be likely to prejudice the security of, or the maintenance of good order and discipline in-

(i) a prison,

(ii) a place of detention provided under section 2 of the Prison Act, 1970,

(iii) a military prison or detention barrack within the meaning of the Defence Act, 1954, or

(iv) Saint Patrick's Institution,

4.6.2 Data subjects (including staff) may be provided with a standard subject access request form (attached) which:
indicates the information required in order to locate the images requested;

a) indicate that a fee will be charged for carrying out the search for the images requested. The maximum fee which may be charged for the supply of copies of data in response to a subject access request is set out in the Data Protection Acts, 1988 and 2003;

b) enquire if a facilitation to simply view recorded images would be satisfactory;

c) indicate that the response will be provided promptly following receipt of the required fee and in any event within 40 days of receiving adequate information.

4.6.3 Staff operating the system shall be able to explain to members of the public the type of images which are recorded and retained, the purposes for which those images are recorded and retained, and information about the IPS's disclosure policy in relation to those images. An information note may be made available as an aid to any such explanation.

4.6.4 The standard subject access request form as provided to an individual shall be accompanied by the CCTV information note (Appendix IV).

4.6.5 All data subject access requests shall be dealt with by a manager or designated member of staff whose identity is known to other staff members (See paragraph 4.1.8).

4.6.6 The manager or designated member of staff must provide a written response to the individual within 40 days of receiving the request setting out their decision on the request.

4.6.7 If the manager or designated member of staff decides that the request will not be complied with, they must set out their reasons in their response to the individual. The reasons for refusal of an access request are down in Sections 4 and 5 of the Data Protection Acts, 1988 & 2003. The specific Section(s) of the Acts which are relied on for not complying with the access request must be notified to the requester[4]. In addition, the requester must be informed of their right to complain to the Data Protection Commissioner.

4.6.8 A copy of the request and response shall be retained and filed securely.

4.6.9 The manager or designated member of staff shall document:

[4] Same as footnote 3 on page 8

a) the request from the individual;

b) the original decision;

c) their response to the request from the individual;

d) the reasons for rejection, if applicable.

4.6.10 In the event that a request is granted, the manager or designated member of staff shall locate the images requested.

4.6.11 The manager or designated member of staff shall determine whether disclosure to the individual would entail disclosing images of third parties.

4.6.12 If third party images are not to be disclosed, as in Section 4.6.11, the manager or designated member of staff shall arrange for the third party images to be disguised or blurred.

4.6.13 If the system does not have the facilities to carry out the type of editing required at (4.6.12) above, a third party or company may be hired to carry out this work.

4.6.14 If a third party or company is hired to carry out the type of editing required at (4.6.12) above, then the manager or designated member of staff shall ensure that:

a) there is a contractual relationship between the Governor and the third party or company;

b) that the third party or company has given appropriate guarantees regarding the security measures they take in relation to the images;

c) The Governor shall have in place appropriate and adequate procedures to ensure those guarantees are met including a right of access to the contractor's premises or systems;

d) The written contract makes it explicit that the third party or company can only use the images in accordance with the instructions of the manager or designated member of staff;

e) The written contract makes the security guarantees provided by third party of company explicit.

4.6.14 It is the responsibility of the Governor to ensure that all staff are aware of an individual's rights under relevant Data Protection legislation as well as those mentioned under this policy.

4.7 Miscellaneous date subject rights

4.7.1 All staff involved in operating the CCTV equipment must be able to recognise a request from an individual to:

a) rectify or edit, where appropriate, personal data.

b) prevent processing likely to cause substantial and unwarranted damage to that individual, unless a legitimate reason exists for such processing.

4.7.2 All staff must be aware of the identity of the manager or designated member of staff who is responsible for responding to such requests.

4.7.3 In relation to a request for rectification, editing or to prevent processing likely to cause substantial and unwarranted damage, the manager or designated member of staff's response should indicate whether he or she will comply with the request or not.

4.7.4 The manager or designated member of staff must provide a written response to the individual within 40 days of receiving the request setting out their decision on the request.

4.7.5 If the manager or designated member of staff decides that the request will not be complied with, they must set out their reasons in their response to the individual.

4.7.6 A copy of the request and response should be retained and filed securely.

4.7.7 The manager or designated member of staff shall document:

a) the request from the individual;

b) the original decision;

c) their response to the request from the individual;

d) the reasons for rejection, if applicable.

4.7.8 Monitoring compliance with this policy

It is the responsibility of the Governor to ensure that there is full compliance with this Policy. Contravention of a provision of the Data Protection Acts 1988 and 2003 may expose a person to prosecution under the Act.

4.8 Monitoring standards

4.8.1 The contact person indicated on the sign should be available to members of the public during office hours. That contact person should be aware of the policies and procedures governing the use of the IPS CCTV equipment.

4.8.2 Enquirers should be provided on request with one or more of the following:

a) the information note, if available, for the purpose of general information which enquirers may receive when they make a subject access request;

b) a copy of this Policy;

c) a data subject access request form if required or requested;

d) the complaints procedure to be followed if an enquirer has concerns about the use of the system;

e) the complaints procedure to be followed if an enquirer has concerns about non-compliance with the provisions of this policy;

f) no fee may be charged in respect of the provision of any of the above documents.

4.8.3 A complaints procedure should be clearly documented by the Governor.

4.8.4 A record of the number and nature of complaints or enquiries received should be maintained by the Governor together with an outline of each action taken.

4.8.5 A report on those numbers should be collected by the manager or designated member of staff in order to assess public reaction to, and opinion of, the use of the system.

4.8.6 A manager or designated member of staff should undertake regular reviews of the documented procedures to ensure that the provisions of this Policy are being complied with. An audit shall be carried out, at least, on an annual basis.

4.8.7 A report on those reviews should be provided to the Director General in order that compliance with legal obligations and provisions of this Policy can be monitored.

4.8.8 An internal annual assessment should be undertaken which evaluates the effectiveness of the system. The audit referred to at (4.8.6) may form part of such an assessment.

4.8.9 The results of the report should be assessed against the stated purpose of the scheme. If the scheme is not achieving its purpose, it should be reviewed or modified where necessary.

4.9 Data Retention/Deletion

4.9.1 All recorded footage will be retained locally for 31 days, unless it is saved to the IPS Storage Area Network (SAN).

4.9.2 All incidents saved to the IPS SAN will be retained for 12 months initially. After the 12 months have elapsed the footage is reviewed and is dealt with in one of the following 2 ways:

a) If the footage relates to an incident that is deemed to be still active, then it is retained for a further 12 months on the SAN and will be reviewed again at the end of that period.

b) If the footage is deemed no longer relevant, it is archived off to tape. This tape is retained for the following 3 years in a secure cabinet. Any footage that is required from the tape during the 3 year period will be restored to the SAN and dealt with as outlined in 1 above. The footage that remains on the tape after the 3 years have elapsed will be automatically deleted (without further reference back to the Governor/Director of Operations).

4.9.3 The 12-monthly review will only concern footage that is 12 months or more on the SAN. This review needs to be carried out by representatives of Legal and Professional Standards Unit, State Claims Agency, Operations Directorate and HR Directorate.

5. Related policies and documents

This Policy should be read in conjunction with:

PIN 015 Irish Prison Service Covert CCTV Surveillance policy (Appendix IV)

PIN 018 Irish Prison Service Information Gathering policy.

6. Definitions

CCTV – Closed Circuit Television

IPS SAN - Irish Prison Service Storage Area Network.

Appendices

Appendix I – CCTV Access Request Form

Appendix II – CCTV Randomiser

Appendix III – CCTV Sign off sheet

Appendix IV – Covert CCTV Surveillance policy

Appendix V – CCTV Information note

Appendix I – CCTV Access Request Form

Governor	
Institution	
Person wishing to access CCTV footage	
Address	
Personal or Third Party request?	
If request from Third Party please outline the reason for request. If from An Garda Síochána, requests should be authorised at Superintendant level.	
Event, to include date, time, location and parties involved.	
Request to view or review and copy?	

Signature Person wishing to access CCTV footage		Date	

Appendix II – CCTV Randomiser

IT Directorate have set up an application to generate at random a 20 minute timeslot for which retrospective viewing of CCTV is permissible. Basically the night shift is broken down into 20 minute time slots and a table containing these timeslots is fed into the Cognos system. The Cognos system then uses its random functionality to select one of these time slots and email it out to the appropriate mail recipient in the prison. This procedure is repeated for each prison, so that we end up with a different timeslot for each institution.

Appendix III – CCTV Sign off sheet

This sheet must be completed before any images can be placed onto the CCTV management software operated on Irish Prison Service sites.

The image below is presented to you for your acceptance. By accepting it, you agree that it will be operated under the guidelines set out in the IPS CCTV policy, (Policy Index No. 007).

Camera number: _____

Camera name: _____

Accepted by the Governor: _____

Date: _____

Appendix IV – Covert CCTV Surveillance policy (Policy PIN 015)

1. Aim

1.1 To provide a clear, consistent and best practice approach to covert CCTV surveillance.

2. Purpose of this policy

2.1 This policy sets out conditions for use of covert CCTV surveillance.

3. Scope of this policy

3.1 This policy applies to all permanent and temporary staff members, independent contractors, subcontractors or any person with covert CCTV surveillance responsibilities.

3.2 All persons involved in the planning, supervision or operation of a covert CCTV surveillance operation should be familiar with this policy.

4. Procedures for implementation

4.1 Overt monitoring is a feature of the everyday prison environment but however, in exceptional circumstances, covert surveillance may be used as part of a specific investigation. Covert surveillance is where CCTV recording equipment is used, and those being monitored are unaware that this is taking place.

4.2 Covert surveillance will only be permitted on a case by case basis, where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies an actual involvement of An Garda Síochána or an intention to involve An Garda Síochána. Advance approval of the Director of Operations is required for any covert CCTV surveillance operation. Any request for the use of covert CCTV surveillance is subject to the IPS Framework for Information Gathering policy.

4.3 Covert surveillance may only be undertaken for a limited but reasonable period of time and consistent with documented objectives. If no evidence is obtained within a reasonable period, the surveillance should cease.

4.4 Only specific (and relevant) individuals/locations may be recorded.

4.5 If the surveillance is intended to prevent crime, overt cameras may be considered as a more appropriate measure, and less invasive of individual privacy.

4.6 Covert surveillance can only take place in accordance with the documented authorisation of the Director of Operations. To justify such surveillance there must be reasonable cause to suspect that unauthorised or illegal activity is taking place, or is about to take place, or that a serious breach of IPS policies and procedures is taking place, or is about to take place.

4.7 A Governor requesting authorisation for covert CCTV surveillance must satisfy the Director of Operations that the action is necessary for the prevention or detection of crime or the prevention of disorder and is proportionate to the nature of the alleged offending.

4.8 Necessity.

This requires that the proposed activity is vital for the effective delivery of the investigation and there is no other means of investigation available that involves a more limited invasion of the subject's privacy.

4.9 Proportionality.

This requires that a balance is taken between the level of intrusion into a subject's privacy and the public interest in addressing the unlawful activity involved and it must be manifestly demonstrated that the public interest outweighs the right to privacy.

4.10 All decisions relating to the use of covert CCTV surveillance will be fully documented.

4.11 Access to recordings from a covert CCTV surveillance event must be tightly controlled to ensure privacy of persons and security of evidence. Footage from covert cameras may only be used for purposes as authorised.

4.12 A manager or designated person shall be nominated by the Governor as Data Protection Officer, who will have responsibility for ensuring the proper, efficient and orderly day-to-day operation of the CCTV system. This person will also be responsible for access requests under the Data Protection Acts, whether for CCTV images or for other personal data held on computer or manual files.

4.13 The governor shall maintain an appropriate record of the system's effectiveness in consultation with prison managers and the Director of Operations.

Appendix V – CCTV Information note.

IPS CLOSED CIRCUIT TELEVISION (CCTV)

INFORMATION NOTE

Closed circuit television is an important and essential system that is in place in and around the prison estate to assist in maintaining the good order and security of the institutions. It is of crucial importance in order to ensure confidence in the operation of CCTV systems that there is no improper use of the equipment. Any misuse of CCTV systems is likely to damage the positive perception of CCTV in the eyes of stakeholders.

All staff members are to make themselves familiar with the contents of this policy and the associated policy.

Respect for the individual's liberty and privacy is a primary consideration in this policy.

The Irish Prison Service will ensure that:

- Signs are placed so that members of staff, inmates, visitors and other stakeholders are aware that they are entering an area which is covered by a CCTV system. These signs are to be clearly visible and legible. Signs will contain the following information:
    - the identity of the person or organisation responsible for the CCTV scheme.
    - the purposes of the scheme, as per Section 4.1.1 of the Policy for CCTV Systems in the Irish Prison Service.
    - details of who to contact regarding the scheme.
- Members of staff are aware by means of Governor's Orders that they may be monitored in a general way and that footage may be subject to limited review, as directed by the Director of Operations, to ensure that required tasks are being carried out to agreed standards.
- In the event of an incident there will be a full review of all relevant CCTV footage.
- Inmates, visitors and other stakeholders are aware by means of appropriate signage that they may be monitored in a general way and that footage may be reviewed in the event of an incident and on a regular basis to ensure that good order is being maintained.

- Only persons authorised by the Governor shall be permitted access to the control area where monitoring takes place. In this regard, the Governor will ensure that at all times entry/exit records to the control area are maintained.
- It will at all times ensure the proper and responsible operation of the CCTV system under its control and further ensure that all persons operating or monitoring the system are appropriately trained in the system's use and understand the restrictions and legal obligations imposed upon them by the laws in this area.
- All uses of the system are appropriate, proportional and in the interest of maintaining good order and security in prisons. CCTV footage may be reviewed regularly, on a sample[5] randomised basis, to ensure good order and security is maintained.
- A manager or designated person will be nominated by the Governor to have responsibility for ensuring the proper, efficient and orderly day-to-day operation of the CCTV system.
- Images are stored securely and for no longer than 31 days, unless required for a specific purpose as per Section 4.9 of the policy under 'Data Retention/Deletion'.
- The Governor shall maintain an appropriate record of the images recorded, the reason for the recording, who may have access to the recording, how long it is to be retained and confirm that it has been disposed of in accordance with procedures when no longer required.
- The Governor shall review the system's effectiveness regularly.

Copies of the policy, Information Note and Standard Subject Access Request Form (see Appendix I of the policy) are available from the Governor.

END OF DOCUMENT

[5] It is envisaged that a sample would not exceed 20 minutes per shift, as outlined in Section (4.1.2)