CODE OF PRACTICE

For the Operation of

HIGHLAND PUBLIC SPACE CCTV NETWORK

The Highland Council

In Partnership with

Police Scotland
(Highland Division)

August 2009
(last update: November 2013)

1

Index

Section 8: Assessment of the network and the code

8.1 System audits
8.2 System evaluation
8.3 Reports
8.4 Changes to the code and procedure manual

Section 9: Human Resources

9.1 Staffing of the monitoring rooms and those responsible for the operation of the network
9.2 Discipline

Section 10: System maintenance and health and safety

10.1 Maintenance of the network
10.2 Future replacement of obsolete equipment
10.3 Installation of other equipment on Police premises
10.4 Health and safety

Appendix

Appendix A – Administration
Appendix B – Camera schedule
Appendix C – Extracts from Data Protection Act 1998
Appendix D – National Standards for Release to Third Parties
Appendix E - Regulation of Investigatory Powers (Scotland) Act
Guiding principles
Appendix F – Access to Information

Definitions

'CCTV'	Closed Circuit Television
'Code'	Code of Practice for the Operation of the Highland Public Space CCTV Network
'Network'	Highland Public Space CCTV Network
'Owner'	The Highland Council
'Network manager'	Nominated representative of the network's owner responsible for day-to-day managing of the network
'Data controller'	The person who (either alone or jointly or in common with other Persons) determines the purposes for which and the manner in which any personal data are to be processed.
'Data processor'	The person who processes the data on behalf of the data controller(s).
'Processing'	Refers to obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.
'DPA'	Data Protection Act 1998
'Partnership'	CCTV partnership between the Highland Council and Police Scotland (Highland Division)
'Recorded material'	Refers to any material recorded by, or as the result of, technical equipment, which forms part of the network, but specifically includes images recorded digitally, or on disc or by way of copying from disc, including digital prints.
'Digital print'	Refers to a copy of an image or images which already exist on digital hard-drive / computer disc.

‘CCTV operator’ Any members of staff working on the network

Section 1: About this code

1.1. Purpose of the code
The purpose of this document is to state the intention of the Highland Council, Police Scotland (Highland Division) and all the other parties involved in the Highland Public Space CCTV Network, to support the objectives of the network and to outline how it is intended to do so. The recommendations in this code are all based on the legally enforceable data protection principles.

This codes purpose is to:

- Ensure that those capturing CCTV images comply with Data Protection Act and other relevant legislation
- Ensure that the images that are captured are usable
- Reassure those whose images are being captured

This code applies only to the Highland Public Space CCTV Network.

1.2 Procedure manual
This code is supplemented by a separate ‘procedure manual’, which offers instructions on all aspects of the day-to-day operation of the network. To ensure the purpose and principles of the network are realised, the procedure manual is based and expands upon the contents of this code.

Section 2: Highland Public Space CCTV Network

2.1 Introduction
The Highland Public Space CCTV Network currently comprises a number of cameras installed at 9 locations, which are Inverness, Wick, Thurso, Invergordon, Tain, Dingwall, Muir of Ord, Fort William and Nairn.

Detailed list of all the Highland Public Space CCTV cameras is included in Appendix B.

2.2 Administration
2.2.1 The Highland Public Space CCTV Network has evolved from the formation of a partnership between The Highland Council and Police Scotland (Highland Division).

- The Highland Council:

  - The owner of the network
  - The manager of the network, with day-to-day responsibility for the network as a whole.

- The Highland Council has the right to delegate its responsibility in part or as a whole to any external contractor.

- Police Scotland (Highland Division):

  - Providing working space in the police stations for CCTV monitoring equipment
  - Operating (including some monitoring duties) the network in those locations and during that time which is not operated by the owner or delegated owner nominee
  - Providing day to day management support.

2.2.2 For the purposes of the Data Protection Act:

- 'Data controller' is the Highland Council and Police Scotland (Highland Division)

- 'Data processor' is any external contractor (monitoring provider) processing the data on the data controller's behalf.

Contact information is listed at appendix A.

2.3 Purpose of the Highland Public Space CCTV Network

2.3.1 The objectives of the network as determined by the partnership, which form the lawful basis for the processing of data are:-

- The prevention and detection of crimes and the enforcement and prosecutions of offenders.
- To enhance community safety.
- To assist the local authority in its enforcement and regulatory functions. ➢ To assist in traffic management.
- To assist in supporting civil proceedings.
- To assist in monitoring any emergency planning operations.

2.3.2 The network will also be used to help train new staff that will be employed in the control rooms within the Highland Council area. A trained and competent person will strictly supervise all training that is undertaken at the CCTV control rooms.

2.4 General Principles of operation

2.4.1 The network will be operated in accordance with all the requirements and the principles of the Human Rights Act 1998.

2.4.2 The operation of the network will also recognise the need for formal authorisation of any covert 'directed' surveillance, 'intrusive' surveillance or crime–trend ('hotspot') surveillance as required by the Regulation of Investigatory Powers Act, Regulation of Investigatory Powers (Scotland) Act 2000 and the police force policy.

2.4.3 The network will be operated in accordance with the Data Protection Act 1998 at all times

2.4.4 The network will be operated fairly, within the law, and only for the purposes for which it was established and are identified within this code, or which are subsequently agreed in accordance with this code.

2.4.5 The network will be operated with due regard to the principle that everyone has the right to respect for his or her private and family life and their home.

2.4.6 The public interest in the operation of the network will be recognised by ensuring the security and integrity of operational procedures.

2.4.7 Throughout this code it is intended, as far as reasonably possible, to balance the objectives of the network with the need to safeguard the individual's rights. Every effort has been made throughout the code to indicate that a formal structure has been put in place, including a complaints procedure, by which it can be identified that the network is not only accountable, but is seen to be accountable.

2.4.8 Participation in the network by any organisation, individual or authority assumes an agreement by all such participants to comply fully with this code and to be accountable under the code.

Section 3: Privacy, Human Rights and Data Protection

3.1 Public concern

3.1.1 It is recognised that operation of the network may be considered to infringe on the privacy of individuals. The partnership recognises that it is their responsibility to ensure that the network should always comply with all relevant legislation, to ensure its legality and legitimacy.

3.1.2 The network will only be used as a proportional response to identified problems and be used only in so far as it is necessary in a democratic society, in the interests of national security, public safety, the economic well being of the area, for the prevention and detection of crime or disorder, for the protection of health and morals, or for the protection of the rights and freedoms of others.

3.1.3 All personal data obtained by the network will be processed fairly and lawfully and, in particular, will only be processed in the exercise of achieving the stated objectives of the network. In processing personal data there will be respect for everyone's right to respect for his or her private and family life and their home.

3.2 Human Rights

3.2.1 The partnership recognises that public authorities and those organisations carrying on functions of a public service nature are required to observe the obligations imposed by the Human Rights Act 1998, and consider that the use of CCTV in the highlands is a necessary, proportionate and suitable tool to help reduce crime, reduce the fear of crime and improve public safety.

3.2.2 This assessment is evidenced by an agreed 'operational requirement' document Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention

or victim welfare. Police Scotland (Highland Division) also consider it as assisting them in carrying out their statutory duties as enshrined in The Police (Scotland) Act 1967.

3.2.3 The codes and observance of the operational procedures contained in the procedure manual will ensure that evidence is secured, retained and made available as required to ensure there is absolute respect for everyone's right to a free trial.

3.2.4 The network will be operated with respect for all individuals, recognising the right to be free from inhuman or degrading treatment and avoiding discrimination on any ground such as sex, race, color, language, religion, political or other opinion, national or social origin, association with a national minority, property or other status.

3.3 Data Protection legislation

3.3.1 The operation of the network has been notified to the Office of the Information Commissioner in accordance with current Data Protection legislation.

3.3.2 The 'data controller' for the network is the Highland Council and Police Scotland (Highland Division).

3.3.3 All data will be processed in accordance with the principles of the Data Protection Act, 1998 that, in summarised form, includes, but is not limited to:

- All personal data will be obtained and processed fairly and lawfully.
- Personal data will be held only for the purposes specified.
- Personal data will be used only for the purposes, and disclosed only to the people, shown within these codes of practice.
- Only personal data which is adequate, relevant and not excessive in relation to the purpose for which the data is held will be held.
- Steps will be taken to ensure that personal data is accurate and where necessary, kept up to date.
- Personal data will be held for no longer than is necessary.
- Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.
- Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information.

3.3.4 Extracts from Data Protection Act 1998 (Section 7 & 8) is included in appendix C.

Section 4: Operation of the cameras

4.1 Cameras and area coverage

4.1.1 The areas covered by CCTV to which this code refers are the public space within the Highland Council authority area.

4.1.2 From time to time transportable or mobile cameras may be temporarily sited within the area. The use of such cameras, and the data produced by virtue of their use, will always accord with the objectives of the Highland Public Space CCTV Network and be governed by this code and manual procedures.

4.1.3 None of the cameras forming part of the network will be installed in a covert manner. Some cameras may be enclosed within ‘all weather domes’ for aesthetic or operational reasons but appropriate signs will identify the presence of all cameras.

4.1.4 Cameras will not be used to look into private residential property. 'Privacy zones' will be programmed into the network (whenever practically possible) in order to ensure that the interior of any private residential property within range of the network is not surveyed by the cameras. Any camera that does not have privacy zones installed will be used with great diligence by trained staff to avoid accidental intrusion of privacy wherever possible

4.1.5 Technical instructions on the use of equipment housed within the monitoring rooms are contained in a separate manual provided by the equipment suppliers.

4.2 Monitoring

4.2.1 The monitoring and recording facilities are located at police stations across the Highland Council authority area (detailed list of all the control rooms included in appendix A).

4.2.2 All CCTV operators receive training relevant to their role in the requirements of the Human Rights Act 1998, Data Protection Act 1998, Regulation of Investigatory Powers Act 2000, Regulation of Investigatory Powers (Scotland) Act 2000, Freedom of Information (Scotland) Act 2002, Private Security Industry Act 2001 and this code and procedures. Further training will be provided as necessary.

4.2.3 In the event that there are no trained operators on site the police duty officer will be authorised to use or instruct an officer to use the network in accordance with the Human Rights Act 1998, Data Protection Act 1998, Regulation of Investigatory Powers act 2000, Regulation of Investigatory Powers (Scotland) Act 2000, Freedom of Information (Scotland) Act 2002 and this code and procedures.

4.2.4 Only those trained and authorised members of staff with responsibility for using the CCTV equipment will have access to the operating controls, those operators have primacy of control at all times.

4.3 Guiding monitoring principles

4.3.1 Any person operating the cameras will act with utmost probity at all times.

4.3.2 The cameras, control equipment, recording and reviewing equipment will at all times only be operated by persons who have been trained in their use and the legislative implications of their use.

4.3.3 Every use of the cameras will accord with the purposes and key objectives of the network and will be in compliance with this code.

4.3.4 Camera operators will be mindful of exercising prejudices, which may lead to complaints of the network being used for purposes other than those for which it is intended. The operators may be required to justify their interest in, or recording of, any particular individual, group of individuals or property at any time by virtue of the audit of the network or by the network manager.

4.4 Monitoring duties

4.4.1 Persons operating the cameras will perform all or part of the duties included below:

- Visually monitor the CCTV screen in the control room for the purpose included in section 2.3
- Record images from selected cameras
- Produce hard copies of recorded images
- Keep all evidential records and witness statements to a standard acceptable under the law of evidence.
- Replay or copy any pre-recorded data at their discretion and in accordance with the code Maintain full management information as to the incidents dealt with by the monitoring room, for use in the management of the network and in future evaluations.
- Maintain a secure system for providing data in accordance with the regulations set up by the owner and Police Scotland (Highland Division).
- Maintain the security of the control room and equipment at all times.
- On detecting an incident closely monitor events on the appropriate monitor, control the camera stations relevant to the incident so as to gain maximum coverage of the scene and details of the incident and to record the incident on the event VCR, notifying the police by telephone using the direct access line.
- Record all incidents in the incident log book.
- Support network manager in reporting faults according to the guidance included in procedure manual.
- And any other duties as designated by the network manager.

4.5 Operation of the network by the police

4.5.1 Under extreme circumstances the police may make a request to assume direction of the network to which this code applies. Only requests made on the written authority of a police officer not below the rank of Inspector will be considered. Any such request will only be accommodated on the personal written authority of the most senior representative of the network owners, or designated deputy of equal standing.

4.5.2 In the event of such a request being permitted, the monitoring room will continue to be staffed, and equipment operated by only those personnel who are authorised to do so, and who fall within the terms of sections 4 and 9 of this code, who will then operate under the direction of the police officer designated in the written authority.

4.5.3 In very extreme circumstances a request may be made for the police to take total control of the network in its entirety, including the staffing of the monitoring room and personal control of all associated equipment, to the exclusion of all representatives of the network owners. Such exclusive control should be communicated to the owner verbally and in writing within 24 hours by a police officer not below the rank of Divisional Commander.

Section 5: Management of recorded material

5.1 Processing and handling of recorded material

5.1.1 Members of the community must have total confidence that information recorded about their ordinary every day activities by the network will be treated with due regard to their individual right to respect for their private and family life.

5.1.2 Every video or digital recording obtained by using the network has the potential of containing material that has to be admitted in evidence at some point during its life span.

5.1.3 All recorded material, whether recorded digitally, in analogue format or as a hard copy digital print, will be processed and handled strictly in accordance with this code and the procedure Manual from the moment they are received by the monitoring room until final destruction. Every movement and usage will be meticulously recorded.

5.1.4 Recorded material will not be copied, sold, released to the public or used for commercial purposes or for the provision of entertainment.

5.1.5 Access to and the use of recorded material will be strictly for the purposes defined in this code only.

5.1.6 Copyright and ownership of all material recorded by virtue of the network will remain with the data controller.

5.2 Recording policy

5.2.1 Subject to the equipment functioning correctly, images from every camera will be recorded throughout every 24-hour period by digital hard-drive. Average retention period is 27 days which varies across all the CCTV control rooms and ranges from 13 up to 49 days since the image has been captured. To enquire about average retention period for each location please contact appropriate police station or the Highland Council Community Safety Officer on 01463 702246.

5.3 Evidential Data

5.3.1 In the event of any Data being required for evidential purposes the procedures outlined in the procedure manual and the Procurator Fiscals instructions will be strictly complied with.

5.3.2 Digital prints will not be taken as a matter of routine. Each time a print is made it must be capable of justification by a member of staff operating the network who will be responsible for recording the full circumstances under which the print is taken in accordance with the procedure manual.

5.3.3 Digital prints contain data and will therefore only be released under the terms of appendix D to this code, ‘Release of data to third parties’. If prints are released to the media, (in compliance with appendix D), in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with the procedure manual.

5.3.4 A record will be maintained of all digital print productions in accordance with the procedure manual. The recorded details will include: a sequential number, the date, time and location of the incident, date and time of the production of the print and the identity of the person requesting the print, (if relevant) and the purpose for which the print was taken.

5.3.5 The records of the digital prints taken will be subject to audit in common with all other records in the network during conducting system audits (outlined in section 8).

Section 6: Accountability and public information

6.1 Public information

6.1.1 A copy of this code will be published on the Highland Council and Police Scotland (Highland Division) website, and a copy will be made available to anyone on request. Additional copies will be lodged at public libraries, some police stations and the Highland Council headquarters, Glenurquhart Road, Inverness and Police Scotland (Highland Division) headquarters, Old Perth Road, Inverness.

6.1.2 For reasons of security and confidentiality, access to the CCTV monitoring rooms is restricted in accordance with this code (see section 7). However, in the interest of openness and accountability, anyone with legitimate reasons wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with the network manager or person(s) delegated by the network manager.

6.1.3 Every individual with any responsibility under the terms of this code and who has any involvement with the network to which they refer, will be required to sign a declaration of confidentiality.

6.2 CCTV signs

6.2.1 Clear and prominent signs will be placed in the locality of the cameras and at main entrance points to the relevant areas, e.g. railway and bus stations to inform the public about the CCTV surveillance being carried out in that particular area. The signs will indicate:

i) The presence of CCTV monitoring; ii) The 'ownership' of the network; iii) Contact telephone number of at least one of the data controllers of the network.

6.3 Complaints procedure

6.3.1 The data controllers will have a clearly documented complaints procedure.

6.3.2 A member of the public wishing to register a complaint with regard to any aspect of the network may do so by contacting any of the data controllers. All complaints shall be dealt with in accordance with the complaints procedure, a copy of which may be obtained from the Highland Council (www.highland.gov.uk) or Police Scotland (Highland Division) (www.scotland.police.uk). The complaint will be dealt with by the appropriate data controller, relevant to the particular case.

6.3.3 The data controller will ensure that every complaint is acknowledged in writing within five working days. The acknowledgement will include advice to the complainant in relation to the enquiry procedure to be undertaken.

6.3.4 In the event of any complaint where satisfaction has not been reached regarding any Data Protection issues, the person making the complaint will be advised to contact the:

Information Commissioner's Office,
Wycliffe House, Water Lane
Wilmslow, Cheshire SK9 5AF
Telephone – 08456 306060 or 01625 545745
Web Address: www.ico.gov.uk

6.4 Request for information - Data Subject Access

6.4.1 Any request from an individual for the disclosure of personal data which he / she believe is recorded by the network will be directed to the data controllers. The data controller will ensure the principles contained within appendix D to this code are followed at all times.

6.4.2 The principles of sections 7 and 8 of the Data Protection Act 1998 (Rights of Data Subjects and others) will be followed in respect of every request; those sections are reproduced as appendix C to this code.

6.4.3 If the request cannot be complied with without identifying another individual, permission from all parties must be considered (in the context of the degree of privacy they could reasonably anticipate from being in that location at that time) in accordance with the requirements of the legislation.

6.4.5 Any person making a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located. Data Subject Access form may be obtained from the Highland Council (www.highland.gov.uk) or Police Scotland (Highland Division) (www.scotland.police.uk) or local police station.

6.5 Exemptions to the provision of information

6.5.1 In considering a request made under the provisions of section 7 of the Data Protection Act 1998, reference may also be made to section 29 of the Act which includes, but is not limited to, the following statement:

6.5.2 Personal data processed for any of the following purposes -

i) The prevention or detection of crime.
ii) The apprehension or prosecution of offenders.
iii) The assessment or collaboration of any taxes or duty or any other crimes on a similar matter.

are exempt from the subject access provisions in any case 'to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection'.

6.5.3 Each and every application will be assessed on its own merits and general 'blanket exemptions' will not be applied.

6.6 Release of data to third parties

6.6.1 Every request for the release of personal data generated by the network will be challenged through the data controller. The data controller will ensure the principles contained within appendix D to this code are followed at all times.

6.6.2 In complying with the national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

- Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this code;
- Access to recorded material will only take place in accordance with the standards outlined in appendix D and this code;
- The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

6.6.3 Members of the police service or other agency having a statutory authority to investigate and / or prosecute offences may, subject to compliance with appendix D, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. Under such circumstances, full details will be recorded in accordance with the procedure manual.

6.6.4 If material is to be shown to witnesses, including police officers, for the purpose of obtaining identification evidence, it must be shown in accordance with appendix D and the procedure manual.

6.6.5 It may be beneficial to make use of footage for the training and education of those involved in the operation and management of the network, and for those involved in the investigation, prevention and detection of crime. Only bona fide training and education courses shall use this information. Recorded material will not be released for commercial or entertainment purposes.

Section 7: Access to and security of monitoring rooms and associated equipment

7.1 Public access

7.1.1 Public access to the monitoring and recording facilities will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the network manager (or delegated representative). Any such visits will be conducted and recorded in accordance with the procedure manual.

7.1.2 Police Scotland (Highland Division) will be entitled to refuse access to any person not involved in the operation or management of the network.

7.1.3 In addition, Police Scotland (Highland Division) will be entitled to determine the suitability of any nominated company or individual employed for the operation or management of the network and shall have the right to refuse access to any persons considered inappropriate.

7.2 Authorised visits

7.2.1 The network manager will have unrestricted access to the CCTV control rooms.

7.2.2 Visits by inspectors or auditors do not fall into the scope of the above paragraph [7.1] and may take place at any time, without prior warning. No more than (two) inspectors or auditors will visit at any one time. Inspectors or auditors will not influence the operation of any part of the network during their visit. The visit will be suspended in the event of it being operationally inconvenient.

7.3.3 The network manager or a person designated by the network manager may authorise the media to be given access to CCTV control rooms. The filming or photography by them of what appears on the CCTV monitor should be confined to wide-angle shots only. No member of the public should be shown in close-up sufficient to identify him/her on screen. Steps should be taken to guarantee the anonymity of CCTV operators in they so wish.

7.3.4 Regardless of their status, all visitors to the CCTV monitoring room, including inspectors and auditors, will be required to sign the visitor's book and a declaration of confidentiality.

7.3 Security

7.3.1 The monitoring room will at all times be secured.

7.3.2 In Addition the CCTV controllers are password protected with only authorised personnel being issued with passwords.

7.3.3 Authorised personnel will be present at all times when the equipment is in use. If the monitoring facility is to be left unattended for any reason it will be secured. In the event of the monitoring room having to be evacuated for safety or security reasons, the provisions of the procedure manual will be complied with.

Section 8: Assessment of the network and the code

8.1 System audits

8.1.1 The network manager (or persons nominated by them) will be responsible for inspecting the operations of the network to ensure that all systems are running and that they adhere to the principles of the code.

8.1.2 System audit will include carrying out technical and data management checks. The technical check shall include a basic assessment of the technical condition of the systems, carried out from the CCTV control room. Data management checks shall include an assessment of compatibility and

usage of the systems as well as include basic support and guidance given to the staff working on the system

8.1.3 Detailed description of duties undertaken during the system audits:

- Check the cameras are recording
- Check the cameras are operational
- Time checks on units and keyboard displays
- Add privacy zones as required and continuously assess the requirement for the privacy zones
- Provide training to the staff working with the systems as per the agreed training programme and identify any other training issues
- Ensure that CCTV images are recorded, stored and retrieved according to this code of Practice
- Undertake informal audits of the paper audit trail
- Ensure that cameras are only being used for appropriate purposes
- Implement and keep up to date the agreed consistent operator procedures included in procedure manual
- Verify the operational readiness of CCTV equipment
- Ensure any staff working on the system are made aware of any amendments to legislation governing CCTV
- Ensure any staff working on the systems is working within current health and safety legislation

8.1.4 System audits will take place at least once per calendar year by no more than two people at any one time. The inspectors will be permitted access to all the CCTV monitoring rooms, without prior notice and to the records held therein at any time, provided their presence does not disrupt the operational functioning of the room. Their findings will be reported to the network manager and Police Scotland (Highland Division) and their visit recorded in the CCTV monitoring room.

8.1.5 Inspectors will be required to sign a declaration of confidentiality.

8.2 Network evaluation

8.2.1 The network will periodically be evaluated to establish whether the purposes of the network are relevant and whether objectives are being achieved. This evaluation will include but not be limited to:-

i) An assessment of the impact upon crime: This assessment shall include not only the immediate area covered by the cameras but the wider town area, the Police Divisional and regional areas and national trends. ii) An assessment of the incidents monitored by the network
iii) An assessment of the impact of the network on city/town center business
iv) An assessment of neighbouring areas without CCTV in relation to areas with CCTV coverage
v) The views and opinions of the public in relation to the operation of the network vi) The operation of the code

vii) Whether the purposes for which the network was established are still relevant viii) Cost effectiveness

8.2.2 The results of the network evaluation will be published on the Highland Council website and will be used to review and develop any alterations to the specified purpose and objectives of the scheme as well as the functioning, management and operation of the network.

8.3 Reports

The annual report on the usage of the network will be published annually by the end of April. A copy of the annual report will be published on the Highland Council website also be made available to anyone requesting it.

8.4 Changes to the code or the procedure manual

8.4.1 Any material amendments to either the code or the procedure manual that will have a significant impact upon the code or upon the operation of the system will take place only after consultation with, and upon the agreement of the owner, Police Scotland (Highland Division) and any external contractor.

8.4.2 A minor change, such as may be required for clarification and will not have a significant impact may be agreed between the owner and Police Scotland (Highland Division) either with or without the agreement of the external contractor.

Section 9: Human resources

9.1 Staffing of the monitoring room and those responsible for the operation of the network

9.1.1 The CCTV rooms will be staffed in accordance with the procedure manual.

9.1.2 Every person involved in the management and operation of the network will be issued with a copy of both the code and the procedure manual. They will be required to sign a confirmation that they fully understand the obligations these documents places upon them and that any breach will be considered as a disciplinary offence. They will be fully conversant with the contents of both documents, which may be updated from time to time, and which they will be expected to comply with as far as is reasonably practicable at all times.

9.1.3 Arrangement may be made for a police liaison officer to be present in the monitoring room at certain times, or indeed at all times, subject to locally agreed protocols. Any such person must also be conversant with this code and associated procedure manual.

9.1.4 All personnel involved with the network shall receive training from time to time in respect of all legislation appropriate to their role.

9.2 Discipline

9.2.1 Any person found misusing the equipment, or the information obtained from the video recording, may be considered to have acted contrary to the Data Protection Act or European Convention on Human Rights, which may subject them to misconduct/litigation procedures.

9.2.2 Every individual with any responsibility under the terms of this code and who has any involvement with the network will be subject to a discipline code. Any breach of this code or of any aspect of confidentiality will be dealt with in accordance with data controller discipline rules.

9.2.3 The data controller will accept primary responsibility for ensuring there is no breach of security and that the code is complied with. Non-compliance with this code by any person will be considered a severe breach of discipline and dealt with accordingly including, if appropriate, the instigation of criminal proceedings.

Section 10: Network maintenance and health and safety

10.1 Maintenance of the network

10.1.1 Equipment associated with the network will only be operated by authorised personnel who will have been properly trained in its use and all monitoring room procedures.

10.1.2 To ensure compliance with the Information Commissioners Code of Practice and that recorded images continue to be of appropriate evidential quality the network shall be maintained in accordance with the requirements of the procedural manual under a maintenance agreement.

10.1.3 Responsibility for maintenance of the network equipment will rest with the owner, which will meet all costs incurred in that respect. Police Scotland (Highland Division) will be entitled to refuse access to any person seeking to undertake maintenance of the equipment. In addition, Police Scotland (Highland Division) will be entitled to determine the suitability of any nominated company employed for the maintenance of the equipment and shall have the right to refuse access to any persons considered inappropriate. The owner must ensure that all persons be required to supply, in advance, sufficient details to allow the necessary checks to be carried out to establish that they are fit and proper persons.

10.1.4 The maintenance agreement will make provision for regular/ periodic service checks on the equipment which will include cleaning of any all weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

10.1.5 The maintenance will also include regular periodic overhaul of all the equipment and replacement of equipment, which is reaching the end of its serviceable life.

10.1.6 The maintenance agreement will also provide for ‘emergency’ attendance by a specialist CCTV engineer on site to rectify any loss or severe degradation of image or camera control.

10.1.7 It is the responsibility of the owner to ensure appropriate records are maintained in respect of the functioning of the cameras and the response of the maintenance organisation.

10.2 Future replacement of obsolete equipment

10.2.1 Responsibility for replacement of obsolete equipment will rest with the owner.

10.3 Health and Safety

10.3.1 Under the Health and Safety at Work Etc. Act 1974, the owner and Police Scotland (Highland Division), for their interest, have certain responsibilities to provide a safe workplace. Where that responsibility relates to visitors or others not employed by the owner or Police Scotland (Highland Division), arrangements will also be in place to ensure that such persons are made aware of:

- Fire precautions
- First aid and accident reporting
- Use of facilities
- Any other reasonable arrangements relating to the premises

10.3.2 Whilst on police premises, any person employed or otherwise engaged by the owner for CCTV purposes, will comply with any arrangements for health and safety within the guidelines of that police, in addition to any other relevant statutory requirement.

10.3.4 Any member of staff working on the network equipment will ensure that any article or equipment supplied by the owner will be used in a safe and proper manner.

10.3.7 All staff working on the network is contractually bound by regulations governing confidentiality and discipline. An individual who suffers damage or distress by reason of any contravention of this code may be entitled to compensation from the relevant data controller.

Appendix A

Network administration

- **Network owner and manager**

The Highland Council
Highland Council Headquarters Glenurquhart Road
Inverness
IV3 5NX

➢ **Police Scotland (Highland Division)**

Old Perth Road
Inverness
IV3 2SY

➢ **CCTV Control Rooms**

- Inverness Area Command Police Station, Burnett Road, Inverness, IV1 1RL
- Nairn Police Station, 69 King Street, Nairn, IV12 4BQ
- Fort William Police Station, High Street, Fort William, PH33 6EE
- Dingwall Police Station (for Dingwall & Muir of Ord), Bridaig, Dingwall, IV15 QH
- Thurso Police Station, Olrig Street, Thurso, KW14 7JA
- Wick Police Station, Bankhead Road, Wick, KW1 5LB
- Tain Police Station, Victoria Road, Tain, IV19 1AU

Appendix B

Highland Public Space CCTV Network
Camera schedule *– as per November 2013*

Inverness	**Fort William**
Camera 1 Corner of EastGate, Camera 2 25 High/ Inglis Street Camera 3 High Street Camera 4 Castle Street Camera 5 Church St Camera 6 Castle Wynd Camera 7 25 Barron Taylor St Camera 8 Corner of Station Sq Camera 9 Bus Station/ Margaret Street Camera 10 Academy St/Chapel ST Camera 11 Friars Lane Camera 12 10 Bank St Inverness Camera 13 Farraline Park Camera 14 Middle of the Market Brae Steps Camera 15 Corner of Ardconnel St/Charles St Camera 16 Church St /Fraser St Camera 17 32 Academy Street Camera 18 Friars Bridge Underpass Camera 19 Victoria Market Camera 20 Victoria Market Church St Entrance Camera 21 Shore St Roundabout Camera 22 33 Grant St Camera 23 54 Grant St/Lochalsh Rd Camera 24 Chapel St Funeral Property Camera 25 Strothers Lane Camera 26 Middle of Stephen's Brae Camera 27 Top of Stephens Brae corner of Arconnel Terrace Camera 28 Leyton Drive, Hilton Camera 29 Hilton Community Centre Camera 30 Hilton Community Centre Camera 31 Hilton Community Centre Camera 32 Hilton Community Centre Camera 33 Ness Walk / Ardross Street Camera 34 Young Street / Huntly Street Camera 35 Young Street / King Street Camera 36 Middle of Raining Stairs Camera 37 Middle of Academy Street Camera 38 Rose Street Car Park Camera 39 Travelling Persons Site Camera 40 Union Street / Church Street	Camera 1 Sherriff Court House Camera 2 High Street- House of Clanjamfrie Camera 3 Bypass (A82) Camera 4 Queen Anne house Camera 5 High Street Camera 6 D.E. Shoes Camera 7 Rear of Post office Camera 8 Viewforth Car park Camera 9 Tesco Camera 10 Alexandra Hotel Camera 11 Morrison's (supermarket) Car park Camera 12 Inside Train Station Camera 13 An Aird Camera 14 A82/A830 Junction Camera 15 Health centre Camera 16 Co-op Caol Camera 17 Kilmalie Road Camera 18 Caol Shopping Centre Camera 19 Kennedy Road / Henderson Road Camera 20 Kennedy Road / Morven Place Camera 21 Kennedy Road / Bruce Place Camera 22 Underpass front Camera 23 Underpass inside
Tain	**Thurso**
Camera 1 Stafford Street / Kings Street Camera 2 Market Street / Queen Street Camera 3 High Street / ST Duthus Street Camera 4 High Street / Castle Brae Camera 5 High Street / Post office Camera 6 Ross Street Camera 7 Geannies Street / Ankerville Road	Camera 1 Royal Bank of Scotland, Beach Road Camera 2 Council Building, back Car Park Camera 3 High Street – Old Woolworth Camera 4 Thurso Precint – Rotterdam Street (bottom half) Camera 5 Thurso Precint – Rotterdam Street (top half) Camera 6 DE's Shop - Trail Street Camera 7 Royal Hotel

Camera 8 Geannies Street / Stafford Street	Camera 8 Pentland Hotel – Princess Street Camera 9 Macae Shop – Princess Street Camera 10 Railway Station Camera 11 A9 at Bridgend Camera 12 Old St. Peters Kirk
Nairn Camera 1 Caword Road Camera 2 Above Boots High Street Camera 3 High Street Camera 4 High Street Camera 5 Corner Harbour Rd A96 Camera 6 Outside Waverley Hotel Camera 7 Jackos bar Camera 8 Old Church Hall Camera 9 Harbour Camera 10 Car Park Camera 11 Church past Police Station	**Wick** Camera 1 Railway Station Camera 2 Front of Wick General Hospital Camera 3 DE Shoes at Traffic Lights Camera 4 Camps Bar Camera 5 Albert Street Camera 6 Spare Camera 7 Harrow Hill Camera 8 Cairndhuna Terrace Camera 9 Murchison Street Camera 10 Nicolson Street Camera 11 Huddard Street Camera 12 Harbour Camera 13 Argyle Square Camera 14 Council Office Car park
Invergordon Camera 1 Railway Bridge, Albany Road Camera 2 Front of School, Albany Rd Camera 3 High Street / King Street Camera 4 Cooperative, High Street Camera 5 Forbse Jewellers, High Street	**Dingwall** Camera1 Strathpeffer Rd Camera 2 High Street/Argyle Street Camera 3 Behind High Street Camera 4 Church Street Junction Camera 5 Royal Hotel Junction
Muir of Ord Camera 1 Railway Station Bridge Camera 2 Railway Station Platform Camera 3 Royal Bank of Scotland Camera 4 Tarradale Primary School	

Appendix C

Extracts from Data Protection Act 1998

Section 7

(1) Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled:

(a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.

(b) If that is the case, to be given by the data controller a description of –

(i) The personal data of which that individual is the data subject;

(ii) The purpose for which they are being or are to be processed;

(iii) The recipients or classes of recipients to whom they are or may be disclosed,

(c) To have communicated to him/her in an intelligible form:

(i) The information constituting any personal data of which that individual is the data subject;

(ii) Any information available to the data controller as the source of those data;

(d) Where the processing by automatic means of personal data of which that individual is the data subject for the purposes of evaluating matters relating to him/her such as, for example, his/her performance at work, his/her creditworthiness, his/her reliability or his/her conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him/her, to be informed by the data controller of the Logic involved in that decision taking

(2) A data controller is not obliged to supply any information under subsection (1) unless he/she has received:

(a) A request in writing, and

(b) Except in prescribed cases, such fee (not exceeding the prescribed maximum) as he/she may require.

(3) A data controller is not obliged to comply with a request under this section unless he/she is supplied with such information as he/she may reasonably require in order to satisfy him/herself as to the identity of the person making the request and to locate the information which that person seeks.

(4) Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he/she is not obliged to comply with the request unless:

(a) The other individual has consented to the disclosure of the information to the person making the request, or
(b) It is reasonable in all the circumstances to comply with the request without the consent of the other individual.

(5) In subsection (4) the reference to information relating to another individual includes a reference to information identifying that individual as the source of the information sought by the request; and that subsection is not to be construed as excusing the data controller from communicating so much of the information sought by the request as can be communicated without disclosing the identity of the other individual concerned, whether by omission of names or other identifying particulars or otherwise.

(6) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, regard shall be had, in particular, to:
(a) Any duty of confidentiality owed to the other individual,
(b) Any steps taken by the data controller with a view to seeking the consent of the other individual,
(c) Whether the other individual is capable of giving consent, and (d) Any express refusal of consent by the other individual.

Note: In considering such instances the data controller must effectively also consider the degree of privacy that the third parties might or might not reasonably expect in being at that location at that time.

(7) An individual making a request under this section may, in such cases as may be prescribed, specify that his/her request is limited to personal data of any prescribed description.

(8) Subject to subsection (4), a data controller shall comply with a request under this section promptly and in any event before the end of the prescribed period beginning with the relevant day.

(9) If a court is satisfied on the application of any person who has made a request under the foregoing provisions of this section that the data controller in question has failed to comply with the request in contravention of those provisions, the court may order him/her to comply with the request.

In this section:
'Prescribed' means prescribed by the Secretary of State by regulations;
'The prescribed maximum' means such amount as may be prescribed;
'The prescribed period' means forty days or such other period as may be prescribed; 'the relevant day', in relation to a request under this section, means the day on which the data controller receives the request or, if later, the first day on which the data controller has both the required fee and the information referred to in subsection (3).
(10) Different amounts or periods may be prescribed under this section in relation to different cases.

Note : These extracts are for initial direction and guidance only. To ensure compliance with the legislation the relevant Data Protection legislation should be referred to in its entirety. Copies of the act and the Information Commissioners code of Practice can be downloaded from their website www.dataprotection.gov.uk

Section 8

(1) The Secretary of State may by regulations provide that, in such cases as may be prescribed, a request for information under any provision of subsection (1) of section 7 is to be treated as extending also to information under other provisions of that subsection.

(2) The obligation imposed by section 7(1)(c)(i) must be complied with by supplying the data subject with a copy of the information in permanent form unless:

(a) The supply of such a copy is not possible or would involve disproportionate effort, or

(b) The data subject agrees otherwise;

(c) And where any of the information referred to in section 7(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

(3) Where a data controller has previously complied with a request made under section 7 by an individual, the data controller is not obliged to comply with a subsequent identical or similar request under that section by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(4) In determining for the purposes of subsection (3) whether requests under section 7 are made at reasonable intervals, regard shall be had to the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

(5) Section 7(1)(d) is not to be regarded as requiring the provision of information as to the logic involved in decision-taking if, and to the extent that, the information constitutes a trade secret.

(6) The information to be supplied pursuant to request under section 7 must be supplied by reference to the data in question at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.

(7) For the purposes of section 7(4) and (5) another individual can be identified from the information being disclosed if he/she can be identified from that information, or from that and any other information which, in the reasonable belief of the data controller, is likely to be in, or to come into, the possession of the data subject making the request.

Note: These extracts are for initial direction and guidance only. To ensure compliance with the legislation the relevant Data Protection legislation should be referred to in its entirety. Copies of the

act and the Information Commissioners code of Practice can be downloaded from their website www.dataprotection.gov.uk

Appendix D

National Standards for the release of data to Third Parties

1. Primary Request To View Data

a) Primary requests to view data generated by a CCTV System are likely to be made by third parties for any one or more of the following purposes:
   i) Providing evidence in criminal proceedings ii) Providing evidence in civil proceedings or tribunals
   iii) The prevention of crime
   iv) The investigation and detection of crime (may include identification of offenders) v) Identification of witnesses

b) Third parties, which are required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:
   i) Police (1)
   ii) Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc.) iii) Solicitors (2) iv) In civil proceedings (3)
   v) Accused persons or defendants in criminal proceedings (3)
   vi) Other agencies, (which should be specified in the Code of Practice) according to purpose and legal status(4).

c) Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:
   i) Not unduly obstruct a third party investigation to verify the existence of relevant data.
   ii) Ensure the retention of data which may be relevant to a request, but which may be pending application for, or the issue of, a court order or subpoena. A time limit shall be imposed on such retention, which will be notified at the time of the request.

Note : A time limit could apply providing reasonable notice was issued to the agent, prior to the destruction of the held data, (e.g. a time limit was about to expire).

d) In circumstances outlined at note (3) below, (requests by accused persons or defendants) the data controller, or nominated representative, shall:
    i) Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.
    ii) Treat all such enquiries with strict confidentiality.

Notes

(i) The release of data to the police is not to be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc. (It may be appropriate to put in place special arrangements in response to local requirements).

(ii) Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, is required to give relevant information in writing prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena. A charge may be made for this service to cover costs incurred. In all circumstances data will only be released for lawful and proper purposes.

(iii) There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation.

(iv) The data controller shall decide which (if any) "other agencies" might be permitted access to data. Having identified those ‘other agencies’, such access to data will only be permitted in compliance with this Standard.

(v) The data controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified to the nearest ½ hour)

2. Secondary Request To View Data

a) A ‘secondary’ request for access to data may be defined as any request being made which does not fall into the category of a primary request. Before complying with a secondary request, the data controller shall ensure that:
    i) The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection Act 1998, Human Rights Act 1998, section 163 Criminal Justice and Public Order Act 1994, etc.); ii) Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act 1998);
    iii) Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck) and
    iv) The request would pass a test of ‘disclosure in the public interest’(1).
b) If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall be put in place before surrendering the material:

i) In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Code of Practice(2).

ii) If the material is to be released under the auspices of 'public well being, health or safety', written agreement to the release of material should be obtained from a senior officer within The Highland Council. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV System Code of Practice.

c) Recorded material may be used for bona fide training purposes such as police or staff training. Under no circumstances will recorded material be released for commercial sale of material for training or entertainment purposes.

Note:

(1) 'Disclosure in the public interest' could include the disclosure of personal data that:

i) Provides specific information which would be of value or of interest to the public

well being

ii) Identifies a public health or safety issue iii) Leads to the prevention of crime

(2) The disclosure of personal data that is the subject of a 'live' criminal investigation would always come under the terms of a primary request, (see III above).

3. Individual Subject Access under Data Protection legislation

1) Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:

i) The request is made in writing;

ii) A specified fee is paid for each individual search;

iii) The data controller is supplied with sufficient information to satisfy him or her self as to the identity of the person making the request;

iv) The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information, which that person seeks, (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement);

v) The person making the request is only shown information relevant to that particular search and which contains personal data of her or him self only, unless all other individuals who may be identified from the same information have consented to the disclosure;

b) In the event of the data controller complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased). Under these circumstances an additional fee may be payable.

c) The data controller is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided, however every effort should

be made to comply with subject access procedures and each request should be treated on its own merit.

d) In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:
    i) Not currently and, as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation;
    ii) Not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings;
    iii) Not the subject of a complaint or dispute which has not been actioned; iv) The original data and that the audit trail has been maintained; v) Not removed or copied without proper authority;
    vi) For individual disclosure only (i.e. to be disclosed to a named subject)

4. Process of Disclosure:

a) Verify the accuracy of the request.
b) Replay the data to the requestee only, (or responsible person acting on behalf of the person making the request).
c) The viewing should take place in a separate room and not in the control or monitoring area. Only data which is specific to the search request shall be shown.
d) It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen).
e) If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requestee.

Note: The Information Commissioners Code of Practice for CCTV makes specific requirements for the precautions to be taken when images are sent to an editing house for processing.

5. Media disclosure

Set procedures for release of data to a third party should be followed, If the means of editing out other personal data does not exist on-site, measures should include the following;

a) In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' shall be followed. If material is to be released the following procedures shall be adopted:

i) The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use.

ii) The release form shall state that the receiver must process the data in a manner prescribed by the data controller, e.g. specific identities/data that must not be revealed. iii) It shall require that proof of any editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection legislation and the System's Code of Practice).

iv) The release form shall be considered a contract and signed by both parties.

8. Principles

In adopting this national standard for the release of data to third parties, it is intended, as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles:

a) Recorded material shall be processed lawfully and fairly and used only for the purposes defined in the Code of Practice for the CCTV scheme;

b) Access to recorded material shall only take place in accordance with this Standard and the Code of Practice;

c) The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

Appendix E

Regulation of Investigatory Powers (Scotland) Act Guiding principles

Advice and Guidance for Control Room Staff and Police Inspectors in respect of CCTV and the Regulation of Investigatory Powers (Scotland) Act 2000.

The Regulation of Investigatory Powers (Scotland) Act 2000 relates to surveillance by the Police and other agencies and deals in part with the use of directed covert surveillance. Section 26 of this act sets out what is Directed Surveillance. It defines this type of surveillance as:-

Subject to subsection (6), surveillance is directed for the purposes of this Part if it is **covert** and is undertaken-

(a) for the purposes of a specific investigation or a specific operation;

(b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

(c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance

The impact for staff in the Police control rooms and CCTV monitoring centres, is that there might be cause to monitor for some time, a person or premises using the cameras. In most cases it will be an immediate response to events or circumstances, as described in section c above. In this case, it would not require authorisation unless it were to continue for some time. The code says some hours rather than minutes.

In cases where a pre-planned incident or operation wishes to make use of CCTV for such monitoring, an authorisation will almost certainly be required. Slow time requests are authorised by a Superintendent or above. If an authorisation is required immediately, an Inspector may do so. The forms in both cases must indicate the reason and should fall within one of the following categories:-

An authorization for directed surveillance may only be granted if it is necessary-

(a) for the purpose of preventing or detecting crime or of preventing disorder;
(b) in the interests of public safety;
(c) for the purpose of protecting public health;

In cases where there is doubt as to whether an authorisation is required or not, it may be prudent to obtain the necessary authority verbally and then in writing by way of the forms. Any authority given should be recorded appropriately for later reference. This should include the name of the officer authorising. Forms should be available at each CCTV monitoring centre and re included in the procedural manual and available from the CCTV User Group Website

Examples:

Insp. Authorisation

An example of a request requiring Inspector authorisation might be where a car is found in a car park late at night and known to belong to drug dealers. The officers might task CCTV to watch the vehicle over a period of time to note who goes to and from the vehicle.

Supt Authorisation

Where crime squad officers wish to have a shop premises monitored from the outside, which is suspected of dealing in stolen goods over a period of days.

No Authorisation

Where officers come across a local drug dealer sitting in the town centre/street and wish to have the cameras monitor them, so as not to divulge the observation taking place.

Appendix F

Access to Information

To request a copy of personal data held on the Highland Public Space CCTV, please complete the **Subject Access Form (PDF)**.

http://www.scotland.police.uk/access-to-information/data-protection/

Please provide as much detail as possible when completing the form, including the date, time and location of when your image was captured, together with a description of what you were wearing and a photograph, which will enable us to locate the footage.

Once you have completed the form, you need to return it to the address below, along with the fee of £10 and copies of your identification documents.

Data Protection Central Processing Unit
Information Management Unit
Police Scotland
Queen Street
Aberdeen
AB11 1ZA

If you need any further advice or guidance, please do not hesitate to contact the Data Protection central processing unit by calling 01224 305170 or by emailing

Once we have received your completed application, fee and appropriate identification, we will deal with it as soon as possible, but we have a maximum of 40 days to process your request.

General Enquiries regarding the Highland Public Space CCTV

The Highland Council and Police Scotland (Highland Division) welcomes comments, suggestions and questions that you may have around CCTV. If you want to contact the CCTV team, please phone the Community Safety Officer on 01463 702246.