



THE MORAY COUNCIL
Community Safety Partnership

PROCEDURE FOR DEPLOYMENT OF MOBILE CCTV UNITS

Deployment Procedure

CONTENTS

Section	Title	Page
1	Purpose and Principles	3
2	Responsibility and Accountability	3
3	Equipment	3
4	Deployment	
	• Requests	4
	• Authority	4
	• Logistics	4
	• Locations	5
5	Signage	5
6	Request for Information	5
7	Health & Safety	5
8	CD / DVD / Hard Copy Handling and Evidence	6
9	Practical Considerations	6
10	Equipment Maintenance	6
11	Covert Use	6
Appendix I	'Request for Deployment'	
Appendix II	'Site Study and Risk Assessment'	

Deployment Protocol

1. Purpose and Principles

The purpose of the deployment of Mobile CCTV units is for:

- the prevention, investigation and/or detection of crime and antisocial behaviour
- helping to reduce crime, fear of crime and tackling antisocial behaviour
- improve community safety

This will be done in accordance with the Moray Community Safety Strategy, the Moray CCTV Code of Practice and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) Policy.

The main objective of this protocol is to ensure that all deployments of the Mobile CCTV units by The Moray Council Community Safety Partnership are carried out effectively, while remaining in accordance with the law.

Where criminal, antisocial and/or disruptive activities exist, it is the role of CCTV to secure evidence of sufficient quality to permit identification of offences and offenders and therefore enable process through the criminal justice system, enforcement action or other appropriate intervention.

2. Responsibility and Accountability

The principal partners in the deployment and operation of Mobile CCTV units under this initiative will be:

- The Moray Community Safety Partnership
- Grampian Police, Moray Sub Division (Police Control Room)

The authorisation of applications made to deploy the CCTV units will be made jointly by the Antisocial Behaviour Co-ordinator (The Moray Council), Partnership Development Officer (Grampian Police) and CCTV Inspector, Moray (Grampian Police) who will be allocated one vote each.

The Chief Legal Officer, The Moray Council will be the data controller for this equipment.

Unless otherwise stated, all equipment used in connection with the Mobile CCTV units is registered with the Community Safety Department based at The Moray Council and will be operated in accordance with the Home Office and Information Commissioner's guidance.

In the event of any complaint arising from use within the terms of the deployment procedure, principle partners will be jointly responsible for any investigation and outcomes.

3. Equipment

The Community Safety Department have redeployable mobile camera units, which can be used in both overt and covert operations. The overt units can be secured to brackets attached to buildings, poles or lampposts. The covert unit can be placed in buildings or houses where a power supply is available. The fact that the cameras are portable and wireless means there are few constraints on where they can be situated.

The units are high resolution, digital technology that will help to produce high quality, reliable images that can be enhanced and enlarged to improve picture clarity. They will use mobile phone type technology for access so operators will be able to dial up the unit from the central control while police officers, with the use of a laptop, will be able to remotely operate the cameras while on patrol.

For the purposes of this document the deployment of the mobile CCTV in the main will be overt and should not be used in covert operations. However, some situations may arise where a 'covert' gathering of information is required. This eventuality is covered in section 11 in this document.

4. Deployment

Requests for Deployment

All requests for deployment will be made on the form at Appendix I, which must be completed and approved by the principle partners.

Information received from members of the Community Safety Partnership, members of the public and elected members will be collated to assist in identifying 'hotspot' areas. This will ensure that cameras are deployed on an intelligence led basis.

Requests can be made by Community Safety partners but will mainly occur through Community Wardens, Grampian Police Tasking & Co-ordinating Group and Housing.

These requests are to be forwarded to the Community Safety Department for consideration.

Authority

In the first instance all requests for deployment will be collated and prioritised by the Antisocial Behaviour Co-ordinator.

The authorising officers will consider submitted requests and notify the applicant(s) of the decision. Appendix I will be completed in respect of all cases (this can be completed retrospectively where a verbal request has been made due to short notice).

In every case it will be necessary to show that use is necessary to prevent and/or detect crime and/or antisocial behaviour, to improve community safety and that filming of any public areas for this purpose is proportional to the rights to privacy of individuals.

Only when all aspects of this Protocol are satisfied, specifically those sections relating to siting, signage and the 'overt' nature of the system will authorisation be granted

The final decision to authorise deployment will rest with the authorising officers:
Antisocial Behaviour Co-ordinator
Partnership Development Officer
Inspector in charge, CCTV, Grampian Police.

Approval for a deployment will require the majority vote of the three principle partners.

Reviews of deployments will be undertaken after a period of no more than three months and any significant changes in circumstances will require a new application.

Where authority has been given for specific overt deployment or deployments, applicants and/or operators should be aware of the potential consequences of continued use in changed circumstances.

The CCTV Working Party will be kept informed of all deployments of the mobile units and subsequently Elected Members will be informed of all deployments within their area.

Deployment Logistics

Staff members who have been trained and deemed to be competent in its use must only effect any deployment and operation of the Mobile CCTV units.

Physical deployments, where the cameras need fixed in position, will be delegated to the nominated contractor (Scotshield).

The Site study and risk assessment (Appendix II) **MUST** be completed by the authorised user in all cases.

The CCTV signage deployed during an overt operation should be within public view and will not be disguised or hidden in any way.

Cameras **MUST NOT** be directed to where the public has a right to expect privacy e.g. must be kept away from windows, private driveways, gardens, etc.

The camera software has the facility to install privacy zones in areas where it would not be appropriate to monitor. Installing operators should install these zones where appropriate. Once installed, any changes to the zones would be logged by the software. CCTV Operators will periodically check the status of the cameras, including the privacy zones to ensure that legislation is not being breached.

Whenever and wherever the CCTV is deployed, entries will be maintained on the spreadsheet held at the police station in electronic format. This will also include any problems operators had on installation.

When deploying CCTV it is essential to have regard to Health and Safety needs and requirements at all times.

Locations

The mobile CCTV units will be deployed to locations throughout Moray that have been identified as having high levels of antisocial behaviour.

Once nominations are agreed a site survey is to be carried out. Locations must be deemed to be ethically, operationally and personally viable. A risk assessment must identify any risks and what can be done to reduce or remove them.

Only once the survey is complete and the location is deemed appropriate for a deployment shall the authorisation be given.

5. Signage

The Mobile CCTV units will be installed on overt installations with the appropriate signage/wording compliant with the data protection legislation and the details of the principle partners.

Signs should be clearly visible and legible to members of the public. These may be placed in obvious locations within premises or on a suitable mounting agreed with the Moray Council Lighting Department on lighting columns etc within the vicinity of the deployment.

Signs will include the following information:

- identity of the department,
- person or organisation responsible for the deployment,
- the purpose of the deployment,
- contact details for the department person or organisation responsible for the deployment.

There is no prescribed number of signs.

No CCTV sign will be less than A4 in size, although this will only be considered sufficient for eye level pedestrian applications. Bigger versions will be available in a variety of sizes and materials

6. Request for Information

Any request from a member of the public for the disclosure of personal information which he/she believes has been recorded by virtue of the System should be directed to Moray Council Legal Department as per existing signage.

If the request cannot be complied with, without identifying a third party, permission from all parties must be sought or if possible, all other third parties' images should be pixelated from the image

Any individual making such a request must be able to satisfactorily prove their identity and provide sufficient information to enable the data to be located e.g. date, time and location of incident etc.

7. Health & Safety

All staff that use the system are to be reminded of their responsibility to maintain awareness of potential health and safety risks.

Installers and operators **MUST** familiarise themselves with the site study risk assessment (Appendix II) for every location/deployment.

Where additional risks become apparent on site, they should be notified to the applicant without delay.

8. CD/DVD/Hard Copy Handling and Evidence

This **MUST ALWAYS** be in accord with Section 15 of the ACPOS CCTV Code of Practice.

Whenever the equipment is in active use any images will be recorded, unless it is necessary to interrupt the recording process to search for previous images on the hard drive and it is not practical to change over the hard drive to carry out the search.

Any Videotapes, CDs / DVDs produced operationally will be the responsibility of the operator, and a copy log must be completed for each CD / DVD produced. Once the DVD has been completed and is to be used as evidence it is then signed for and passed to the appropriate officer who would lodge the evidence as a police production. At this point the evidence no longer becomes the responsibility of the operator. No recorded images will be copied, sold or otherwise released or used for commercial purposes or for the provision of entertainment.

On the completion of an operation any images which are not used as productions will in all cases be destroyed/overwritten within 31 days of initial recording.

All images are protected under the Data Protection Act. (Section 12)

9. Practical Considerations/Training

Only staff that have completed training and are deemed to be competent in all aspects of the systems operational use, will be permitted to use the CCTV system to gather evidence. This applies to both installers and operators.

10. Equipment Maintenance

Principle partners will be responsible for the care and storage of the CCTV equipment when it is not deployed and will make equipment available for any routine maintenance.

The Community Safety Partnership will be responsible for the costs of routine maintenance, including wear and tear.

The Community Safety Partnership and Grampian Police will be responsible for the equipment when it is in active use, and as such will ensure that the equipment is operated within its operational limits.

The Grampian Police Control Room will hold and maintain a faults record for the system. A copy log and visitors logs to record notable incidents, operating difficulties and or any items of user interest should be completed for each deployment. These logs will be kept for 5 years.

11. Covert Use

Authority may not be granted where the CCTV system is used in the following circumstances:

- a) Covert surveillance either directed or intrusive on individual persons, at residential premises and/or the inside of private vehicles, or where the consequences of surveillance are likely to result in the discovery of confidential information;
- b) Covert surveillance in the course of specific operations or during a specific investigation or in such a manner as is likely to result in obtaining of private information about any person.

The Regulation of Investigatory Powers Act (Scotland) 2000 and published Codes of Practice deal with who should authorise surveillance equipment in these circumstances.

It will only be possible for the CCTV cameras to be used in 'covert' circumstances if users obtain in writing consent from the Chief Legal Officer. The authorisation for use under Regulation of Investigatory Powers Act (Scotland) 2000 is **an additional requirement** to this consent to use the equipment.

There will be NO intrusive surveillance at any time.

An authorisation for directed surveillance is required whenever there is a real possibility that the manner in which it is proposed to carry out particular surveillance will result in the obtaining of private information about any person, whether or not that person is or becomes a subject of the operation

Data Protection Act 1998

All personal data obtained by the CCTV system should be fairly and lawfully processed and in particular, the data shall only be processed in accordance with the stated objectives of the system. In processing the personal data there will be total respect for everyone's right for his or her private and family life and their home.

All data will be processed in accordance with the principles of the Data Protection Act 1998 which are summarised below:

- (1) Personal data shall be processed fairly and lawfully.
- (2) Personal data shall only be held for purposes stated.
- (3) Personal data shall be adequate, relevant and not excessive.
- (4) Personal data shall be accurate.
- (5) Personal data should not be kept for longer than is necessary.
- (6) Personal data shall be processed in accordance with individuals' rights and they will be allowed access to that data and if necessary shall be permitted to correct or erase it.
- (7) Procedures shall be put in place to prevent unauthorised access, alteration, disclosure or loss or destruction of information.
- (8) Personal data should not be transferred to countries without adequate data protection.

**APPLICATION FOR REDEPLOYMENT OF PORTABLE CCTV CAMERA
(OVERT USE ONLY)**

NOTE: If the intended camera activity is concerned with a named individual or is likely to lead to collateral intrusion on the privacy of an individual then the application should be made on CID 11/1 – Application for Directed Surveillance Authority

Name of Applicant		Post	
Station/Dept/Division		OperationName (if app)	
Organisation			
Tel.		Email	

Operational Reason/Necessity
a. Brief details of Investigation/Operation
b. Camera Activity to be undertaken
c. Benefits to be obtained from this activity and why it is necessary
d. Detail any sensitivities in the local community or similar activities by other public authorities which could impact on the deployment

Applicant		Signature	
Date			

Principle Partner Authorisation

APPROVAL	YES	<input type="checkbox"/>	Authorisation for time period of	months starting
	NO	<input type="checkbox"/>		

Detail reasons for support/refusal including any objections raised

ASB Co-ordinator Signature		Date	
Partnership Development Officer Signature		Date	
CCTV Inspector Signature		Date	

Risk Assessment

Ethical – High/Medium/Low (explain rationale for classification)

Personal – High/Medium/Low (explain rationale for classification)

Operational – High/Medium/Low (explain rationale for classification)

Risk Management Plan

Having identified the risks, what action will be taken to remove or reduce them

Print Name:

Signed:

Date: