ABERDEEN CITY COUNCIL

COMMITTEE	Corporate Policy and Performance
DATE	14th June 2012
DIRECTOR	Stewart Carruth
TITLE OF REPORT	Procedure for Close Circuit Television (CCTV)
REPORT NUMBER:	H&E/12/046

1. PURPOSE OF REPORT

To seek Committee approval for the attached Procedure for Close Circuit Television (CCTV) as covered in the report.

2. RECOMMENDATION(S)

1. To approve the procedure.

3. FINANCIAL IMPLICATIONS

There are no financial implications arising from this report.

4. OTHER IMPLICATIONS

Staff must be aware of and be able to implement the Procedure if required. The Procedure will be communicated to staff via training, the Zone, team briefings and any other relevant corporate communication.

The Procedure sits under the the Data Protection policy and has relevance to the ICT Acceptable Use Policy and associated guidelines and reinforces these in relation to the processing of personal (or sensitive personal) information held by the Council. Further, the procedure has been drafted having regard to the Information Commissioner's Code of Practice on CCTV.

Failure to correctly comply with Data Protection legislation could leave the Council exposed to investigation by the Information Commissioner, a monetary penalty or legal action.

5. BACKGROUND/MAIN ISSUES

In order to comply with the Data Protection Act 1998 we are required to have a procedure in place for the use of CCTV within Aberdeen City Council.

As part of the new procedure includes the need for an impact assessment of any system, there is an opportunity for services to determine whether their particular CCTV system is justified and if so to ensure it is being operated appropriately. This, and compliance with the procedure will ensure that the Council is operating and using the images captured on CCTV appropriately.

6. IMPACT

Compliance with the Procedure will help to support the Council's obligations in relation to Data Protection

Public – Equalities and Human Rights Impact Assessments (EHIRA) were undertaken in relation to the Corporate Data Protection Policy and 4 Procedures in 2007. As this is a new procedure, the EHIRA has been updated and is included with the background papers.

7. BACKGROUND PAPERS

Equalities and Human Rights Impact Assessment.

9. REPORT AUTHOR DETAILS

Colin Walker, Antisocial Behaviour Officer, Housing and Community Safety. colinwalker@aberdeencity.gov.uk

Jess Anderson, Senior Solicitor, Commercial and Advice Team, Legal and Democratic Services.
JeAnderson@aberdeencity.gov.uk
01224 52 2553

Procedure

for

CLOSE CIRCUIT TELEVISION (CCTV)

April 2012

CONTENTS

1. INTRODUCTION

This procedure describes the way Aberdeen City Council ("ACC") uses closed circuit television (CCTV) and what use it makes of the images recorded. It has been prepared having regard to the Council's obligations as a "Data Controller[1]" under the Data Protection Act 1998. The procedure is designed to ensure that personal data consisting of images of people picked up by a CCTV system ("data subjects") are processed fairly by ensuring that the data subject is aware:

- Of the identity of the data controller
- The purpose or purposes for which the data are processed; and
- Any further information the data subjects should be given in the interests of fairness.

This procedure sets out the common standards to be adopted by all of ACC staff[2].
A breach of any of the procedure by a member of staff is regarded by ACC as an extremely serious matter. Depending upon the particular circumstances of the breach, such a matter may attract disciplinary proceedings against that member of staff. Where ACC staff deliberately and knowingly breach this procedure, they will be subject to ACC disciplinary procedures, and such matter may be reported to the Police. All ACC staff can access details with respect to ACC disciplinary procedures directly from Human Resources, Corporate Governance.

This procedure will be reviewed on an annual basis and at appropriate intervals in between to ensure that it remains an accurate and useful guide. The Director of Housing and Environment in conjunction with Head of Legal will approve any updates to the procedure and that it will be reviewed annually by the Community Safety Manager or at such time as is necessary to reflect any change in law or practice**.** The next such review will take place in June 2013. The most up-to-date copy of this procedure can be located on the Zone and will be provided to those services that operate CCTV, along with the relevant forms referred to herein.

For the avoidance of doubt and in the event of an apparent contradiction occurring between legislation, policy or best practice, legislation will always take priority. This also applies to any future legislation that may be enacted.

[1] A person who determines the purpose and manner in which personal data are processed.
[2] The term "staff" includes full time, part time, temporary and contract employees.

2 PURPOSE OF THE PROCEDURE

2.1 ACC operates CCTV systems for a number of reasons. Principally such a system can be installed for the prevention, investigation and detection of crime (particularly, but not restricted to, vandalism or the theft of Council property) and the apprehension and prosecution of offenders. A system may also be used to enhance the safety of staff and the public. Whilst not its principal function, CCTV footage may, in appropriate circumstances, be used in connection with staff discipline.

2.2 A CCTV system can, and is, also used to assist in providing a safe environment for all members of the community. CCTV is a surveillance tool which should be used as an integral part of a structured community safety programme. Its main function is to assist crime reduction and CCTV is often installed in public places for this purpose. If maintained appropriately, any footage recorded can assist in the detection of crime and apprehension and prosecution of offenders.

2.3 The Council has a part to play in community safety and will use portable CCTV cameras to tackle local antisocial behaviour issues in conjunction with the police, using intelligence led methodology. The Council also uses CCTV cameras for security purposes in a number of premises it owns for the purpose of public safety and crime reduction, e.g. schools, libraries, entrances to council office premises. In order to maintain public confidence and the confidence of any partnership agencies with whom the Council works, it is vitally important that there is not improper use of any of the CCTV equipment or material recorded thereon. All users of the CCTV monitoring equipment are to pay due regard to the rights of privacy enjoyed by every member of society and no use of the CCTV systems shall compromise this fundamental right, unless this is strictly permissible by law. Particular attention must be paid to the Human Rights Act 1998, the Freedom of Information (Scotland) Act 2002 and the Data Protection Act 1998. Where possible, privacy will be ensured by both technical means in the camera installation and also by requiring confidentiality on the part of the monitoring staff.

2.4 This procedure seeks to provide a comprehensive guide to staff having regard to the responsibilities incumbent on the Council under the aforementioned legislation, so that all business areas within the Council are maintaining and adhering to the same acceptable standards.

The purposes of, which are linked to the Community Plan:

- For crime prevention and community/public safety, and as far as is possible, to allow Aberdeen city to be free from crime, the fear of crime and anti-social behaviour.

  To help secure a safer and healthier environment for those who live in, work in, trade in, and visit the city.

- Assist in the identification, apprehension and prosecution of offenders by providing evidential material to the police to secure successful prosecutions in court.

- Maintain public order, and to provide social and commercial benefits.

3. WHEN TO USE CCTV?

3.1 The use of CCTV can be a privacy issue, because it is capable of recording a person's movements as they go about their day to day activities. You should give careful consideration to whether it's appropriate to use it; the fact that it is possible, affordable or has public support should not be the primary motivating factor. You should take into account what benefits can be gained, whether better solutions exist, and what effect it may have on individuals.

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

3.2 You should consider these matters objectively as part of an assessment of the scheme's impact on people's privacy. This does not have to be an extensive or time-consuming process in all cases. The extent of assessment necessary will depend on the size of the proposed scheme and the level of impact it is likely to have on people's privacy.

You should use the results of this assessment to determine whether CCTV is justified in all the circumstances and if so how it should be operated in practice.

3.3 The things to cover in any impact assessment include:

- What Directorate/ Head of Service in the Council will be using the CCTV images?
- Who will take legal responsibility under the Data Protection Act (DPA)[3]?
- What is the Council's purpose for using CCTV? What are the problems it is meant to address?
- What are the benefits to be gained from its use?

[3] Whilst the Head of Legal and Democratic Services is the Nominated Representative, it is the manager responsible for that system who assumes responsibility for its proper use.

- Can CCTV technology realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Do you need images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?
- Will the particular equipment/system of work being considered deliver the desired benefits now and remain suitable in the future?
- What future demands may arise for wider use of images and how will you address these?
- What are the views of those who will be under surveillance?
- What could you do to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?

3.4 If you are establishing a large system, or considering a use of CCTV which could give rise to significant privacy concerns, you may wish to consider using the ICO's Privacy impact assessment handbook. If this is likely to be the case, please contact the Head of Legal and Democratic Services for advice.

3.5 ACC may use CCTV for the following purposes:
- Crime Prevention and Prosecution of Offenders
- Monitoring security of premises and assets
- Public and employee safety
- Staff discipline
- Parking
- Anti-social behaviour.

3.6 There may be situations where CCTV may be operated by or on behalf of the Council by another body. Where this is the case, the Council will also need to consider wider human rights issues and in particular the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life). This will include:
- Is the proposed system established on a proper legal basis and operated in accordance with the law?
- Is it necessary to address a pressing need, such as public safety, crime prevention or national security?
- Is it justified in the circumstances?
- Is it proportionate to the problem that it is designed to deal with?

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

3.7 Where you are considering contracting with another person[4] to operate CCTV on the Council's behalf, please contact the Head of Legal and Democratic Services for legal advice.

[4] E.g. a legal person; an individual, company or partnership.

4. TECHNICAL SPECIFICATION

4.1 Any CCTV images must be adequate for the purpose for which you are collecting them. It is essential that you chose camera equipment and locations which achieve the purposes for which you are using CCTV. Both permanent and movable cameras should be sited and image capture restricted to ensure that they do not view areas that are not of interest and are not intended to be the subject of surveillance, such as an individual's property. The cameras must be sited and the system must have the necessary technical specification to ensure that images are of the appropriate quality.

4.2 When considering the use of CCTV and having regard to the purpose behind its use, you should have regard to the following;

- The camera location- is it minimising surveillance on areas you aren't requiring it to?
- Setting up the system so it only records at specific times or records movement, if this is appropriate?
- the quality of the footage recorded as a direct consequence of the camera's location,
- is the camera suitable for the location, bearing in mind the light levels, shape and type of camera and the capacity of the camera to cover the area to be surveyed,
- Will the cameras be located somewhere so that they are protected from vandalism?
- Will the system produce images of sufficient size, resolution and frames per second?

4.3 Cameras will not be used to look into private residential properties, the curtilage of same or any other area where a person would have a reasonable expectation of privacy. 'Privacy Zones' shall, where possible be programmed into the system in order to ensure that any private residential properties within range of the system are not surveyed by the cameras.

4.4 If it is not possible to restrict the equipment to avoid images from those spaces not intended to be covered by the scheme, then operators shall be trained in recognising the privacy implications of such spaces being covered. If domestic areas, such as dwelling houses or gardens, border those spaces intended to be covered by the equipment, and there is a possibility that the domestic areas may be recorded, then the Council will consult with the owners and/or residents of such spaces.

4.5 Camera operators will be aware of the purposes for which the system is intended. Operators may be required to justify their interest in, or recording of, any particular individual, groups of individuals or property at any time by virtue of an audit of the system.

4.6 If the equipment being used has sound recording facilities this should not be used to record conversations between members of the public.

4.7 Temporary and Mobile Monitoring Systems and CCTV Dummy Cameras

4.7.1 Mobile and Temporary Monitoring Systems

4.7.2 Mobile and Temporary CCTV Systems may also be used to monitor public spaces. The systems will be deployed at a set location and shall be reviewed every six weeks from the date they are activated at that location. The proposed use of mobile or temporary CCTV Systems shall be taken by Antisocial Behaviour Manager who shall ensure that the systems are removed when they are no longer required.

4.8 CCTV Dummy Cameras

4.8.1 CCTV dummy cameras will not be used under any circumstances, as the use of such cameras will undermine public confidence in the CCTV system.

4.9 Body Worn Cameras

4.9.1 The use of body worn cameras has been authorised by Committee solely for use by City Wardens. The purpose of the cameras is to allow City Wardens to obtain and secure evidence at the scenes of incidents and crimes. When used effectively, body worn cameras can promote public reassurance, improve staff safety while detecting and reducing crime or anti social behaviour.

4.9.2 Any recorded material or footage captured by the body worn camera shall comply with the requirements of this procedure, in so far as it relates to disclosure, monitoring, retention and destruction.

4.9.3

A procedure regarding the operation of the body worn camera shall be read in conjunction with this procedure and both are available to staff on request.

5. USE OF THE CCTV SYSTEM

5.1 The use of the CCTV system will be restricted to the intended purposes outlined above. Managers and operators will pay proper attention to an individual's rights of privacy. Persons who do not have proper authority will not view images.

5.2 ACC's CCTV system is registered with the Information Commissioner in terms of the Data Protection Act 1998. Besides this, a record must be kept (in one document) of all ACC's CCTV systems for audit purposes and this is discussed in more detail in Part 10. This record is kept by the Head of Legal Services,[5].

5.2 Maintenance of the equipment

5.2.1 Both the maintenance contractor and the manager responsible for the CCTV system will keep a log (both an electronic copy and a hard copy) of all repairs and maintenance to all cameras and equipment). The log is available at Appendix 5.

5.2.2 Cameras shall be properly maintained and serviced to ensure that clear images are recorded at all times.

5.2.3 Reasonable precautions shall be taken by the system manager to ensure that cameras are protected from vandalism.

5.2.4 System Operators shall report any damage to cameras, or change in the quality of recording of any camera, to the system manager as soon as reasonably practicable.

5.2.5 Should a camera be recording less clearly than usual, or be damaged in any way, the manager of the system shall ensure that the camera is repaired as quickly as possible, and in any event within 5 working days of the damage becoming known to the manager.

5.2.6 All Officers should carry out and complete a visual and physical check of all CCTV equipment regularly throughout their shift, record and report any defects identified. This is important to ensure that equipment is functioning properly and faults are detected early.

5.3. Daily Checks

5.3.1 Daily Checks require to be completed formally at least once per day and recorded as having been checked in the Daily Work Plan. Faults should be reported on the same day (if a 24 hour reporting service is available) or by the

[5] Please refer to Part 10 for information on the Audit requirements

next working day. There will be a formal Maintenance Contract that includes an annual service.

5.3.2 The daily check is carried out by the nominated member of staff on site responsible for operation, control and maintenance of CCTV and shall:

(a) Carry out a visual check of all CCTV equipment at daily intervals

(b) Identify any defects and report them to the appropriate Contractor, immediately on the same day or by the next working day if there is no 24 hour reporting service.

(c) Record the defect(s) should the Log Book and CCTV maintenance repair log detailing the following date, time and defect.

(d) Where the Contractor visits site, check for proof of identity of Contractor on arrival on site.

If the defects cannot be repaired at that time, then record basic details on the reason for non repair and the likely timescale in the CCTV maintenance repair log and the Log Book.

(e) Ensure CCTV equipment is operational before Contractor leaves site.

(f) Check that recording is now operating.

6 SIGNAGE

6.1 Signs indicating the operation of CCTV will be displayed at the main access points of all premises where CCTV is installed (for both indoor and open space systems), and also in all indoor and outside areas where CCTV either already exists or where it is to be installed. Signs will be placed so that members of the public are made aware, by way of a visible and legible sign, that they are entering a zone which is covered by surveillance equipment. Each sign will include the following information:

a) The owner of the system – “The scheme is controlled by Aberdeen City Council”.

b) The phone number of the person who is managing the system (can be person receiving calls on there behalf) “For further information contact 01224-00000”

c) The reason for CCTV being installed in this area is:

“Images are being monitored for the purposes of crime prevention and

Public Safety".

6.2 The contact number indicated on the sign shall be available to members of the public during normal office hours (9.00am – 5.00pm, Monday to Friday, excluding public holidays). In order to answer any questions (which the public may ask by telephone) all employees (staff) shall be aware of the contact number and this procedure.

See Appendix 1 for template signage.

7 STORING/ VIEWING IMAGES

7.1 All recorded images will be managed strictly in accordance with this procedure.

7.2 Location of the Equipment

7.2.1 The monitoring equipment associated with the CCTV systems will be located within an appropriate secure area and must be in such a position that it cannot be readily viewed by unauthorised persons (e.g. members of the public and staff) and secure when unattended.

7.2.2 Any monitors which display images from areas where individuals have an expectation of privacy must only be viewed by authorised employees.

7.3 Operation of Equipment

7.3.1 Only authorised employees will operate the equipment. To prevent unauthorised use, the keyboard will be locked and the TV monitor will be switched off when the system is not in use.

7.4 Access to Control Rooms/ areas with monitoring equipment

7.4.1 Only authorised personnel will be allowed access to the CCTV control rooms/areas.

7.4.2 Public access to any CCTV control room within Aberdeen City Council will be prohibited except for reasons justifiable by law. Visits will not take place as a matter of routine. Any visiting group or person must have prior permission from the CCTV Systems Manager, who will consider the legal justifications for such a visit.

8 DISCLOSURE OF RECORDED IMAGES

8.1 Disclosure of images to the Police/ Third parties

8.1.1 Third parties, including police officers or solicitors, shall only be allowed access to CCTV recordings in limited circumstances, and in strict accordance with the requirements of the DPA 1998 and the HRA 1998. Under normal circumstances there will be no release of CDs, or video tape images, to third parties.

8.1.2 It is foreseeable that the following third parties will be allowed access to CCTV recordings, in the following circumstances:

- Law enforcement agencies (i.e. the police), where the recording would assist in the investigation of an alleged crime;
- The Procurator Fiscal, when necessary, or when instructed by him/her in connection with the investigation and detection of crime;
- Legal representatives of the relevant parties;
- The media, only in special circumstances where such a release would help in the prevention of crime and resolution of serious crime, and as authorised by the Lord Advocate's guidelines.

Only authorised access will be allowed to recorded CDs, videotapes and other images.

8.1.3 Access to the recordings will be restricted to the manager and designated members of staff. Third parties will only be allowed access to recordings in strict accordance with the requirements of the DPA 1998 and the HRA 1998.

8.1.4 Should access to images be required by the Police, they will require to furnish the Systems Manager with a completed ADM 8/9 form, which has been authorised by a ranking officer. A copy of this form is attached at Appendix 3 for information.

8.1.5 Where a request is received by the Procurator Fiscal, the Systems Manager should also require something in writing from the Fiscal which sets out the reasons why they have determined it's necessary to require the footage/ images etc.

8.2 <u>Disclosure of images to defence agents</u>

8.2.1 By law any relevant evidence seized by the police for use in criminal proceedings must be disclosed to the defence. Ordinarily this evidence will have been logged as a production with the Procurator Fiscal who will arrange for the defence to view these productions. However, in certain areas, local arrangements ensure that the police will organise the examination and viewing of the productions.

8.2.2 Any defence agent viewing or examining recordings or images from public CCTV systems which are Crown productions must be authorised to do so, in writing, by the Procurator Fiscal. This viewing will take place at a location provided by the police or the systems owner.

8.3.3 Where a request is made to the police by a defence agent for access to view recordings and images from an Aberdeen City Council CCTV system, which are Crown productions, such a request will be in writing and in a manner currently existing for arranging precognitions. At the time of viewing the recording or taking the precognitions, the police reporting officer, or other suitable member of staff, will only show the images, after seeing the relevant written permission from the Procurator Fiscal. Copies of CD images, Video images, and/or still prints or other images will not be handed over to the defence agent. The defence agent will only be allowed to view relevant images. Any requests made by defence agents for such facilities should be referred to the police.

8.3.4 If a defence agent requests access to Aberdeen City Council CCTV recordings and images that are not logged as Crown productions this will ordinarily be refused. Defence agents, like all third parties, have no automatic right of access to public CCTV recordings. Access to Aberdeen City Council CCTV recordings by defence agents will only be authorised in strict accordance with the DPA1998 and the HRA 1998. The relevant information (images) will be held in secure storage pending a decision by ACC on the defence agent's access request.

8.4 Disclosure to other Council services

8.4.1 If you receive a request from another Council service for access to any recorded footage, you should pass this request to the Systems Manager who has responsibility for the CCTV system.

8.4.2 The Systems Manager should obtain from the Service requesting the information, clarification on why they need access to the footage and what they are requesting, e.g. it may be excessive to grant access to several hours' worth of footage if they are only interested in footage captured at a certain time.

8.4.3 In granting access to the footage, the Systems Manager has to ensure that the requesting Service has a legitimate aim to view the footage and that's its proportionate to permit access. Where the manager is unsure, s/he should seek legal advice.

8.5 Requests for footage/images under the Data Protection Act 1998

8.51 In terms of section 7 of the DPA 1998, individuals have a right to have access to information which ACC, as a data controller, holds about them, this would include access to any still images of them caught or recorded on a CCTV system.

8.5.2 There are a limited number of exemptions to an individual's right of subject access. One exemption of potential relevance to CCTV images can found at section 29 of the Act. This section provides an exemption from the subject access rights where personal data is held for the purposes of:

(a) Prevention or detection of crime;
(b) Apprehension or prosecution of defenders

ACC will be entitled to withhold footage or images from an individual making a subject access request, where ACC have determined that to disclose the personal data would be likely to prejudice one or both of the above purposes. This judgement must be made on a case by case basis, and in relation to each element of the personal data held about the individual in consultation with the Police, where appropriate.

8.6 Requests for images under the Freedom of Information (Scotland) Act 2002 (FOISA)

8.6.1 FOISA creates a right to information held by a Scottish Public Authority. Whilst images caught by CCTV would be classed as information and therefore be "caught" by such a request, FOISA contains an exemption in section 38 where a request relates to information about individuals. It is likely that should a request be received which relates to information captured on CCTV, it would be exempt under FOISA.

8.6.2 If you receive a written request for CCTV footage, you should consider:

- Are the images those of the requester? If so then that information is exempt from FOISA. Instead this request should be dealt with as a subject access request under clause 8.5 above.
- Are the images of other people? These can be disclosed only if disclosing the information in question does not breach the data protection act or its principles.

If you need further advice on this, please contact the person within your Directorate charged with giving advice on information management. The contact details should be available on the Zone.

8.7 Release of recordings

8.7.1 No CDs, tapes, images or prints will be used for entertainment purposes, nor will they be released to the press, television companies or any other media agencies unless in the special circumstances outlined above.

8.7.2 Occasions may arise whereby images are required by agencies other than those listed above, and in such instances, permission should be sought in writing from the Data Controller, who shall determine such requests on a case by case basis. The relevant recordings shall be held in secure storage pending the Data Controller's decision on the third party request.

8.7.3 All requests for access by third parties shall be fully documented by the operator in accordance with Appendix 6. In particular the date of the request, the name of the party making the request, the outcome of the request and the reason why access was allowed or denied should be documented.

8.8 Copyright

8.8.1 All images recorded by the CCTV systems are the copyright of Aberdeen City ACC, and may not be reproduced in whole or in part without the written permission of the Chief Executive of ACC.

9. Retention of footage/ images

9.1 The DPA 1998 does not prescribe any specific minimum or maximum retention periods which apply to footage recorded on a system. The retention of these images should be a matter for ACC to decide. However, the DPA 1998 does state that a public authority should not keep images/ footage for longer than is necessary.

9.2 Security

It should be demonstrable that access to storage media by either physical or electronic means is sufficiently controlled to prevent unauthorised access. Approved access should be logged to include who did what and when either via an access control system or via an audit trail.

9.3 Data encryption

Data encryption scrambles the digital data that forms an image in such a way that it would be difficult to reconstruct into the original recorded image. Data encryption should not prevent authorised users /organisations from gaining access to playback of the exported images.

9.4 Recording retention

You should not keep images for longer than strictly necessary to meet your own purposes for recording them. On occasion, you may need to retain images for a longer period, where a law enforcement body is investigating a crime, to give them opportunity to view the images as part of an active investigation.

9.5 Storage functionality

The system must be intuitive and assist the user in management of the system. One of the key features that a user requires is the ability to see how much recording they are receiving on a particular site:

a) the Digital Video Recorder (DVR) system should indicate how many days and hours of recording the system has stored.

b) the DVR system should indicate an estimated retention period based on the changing of settings.

9.6 Removable storage media

Where removable media is used as primary storage, care is required in how that physical media is utilised. While the removable media exists within the DVR under controlled access, the digital images on that media may be considered as both the Original Recording and master copy. It should be noted that: a) should the media be removed for evidential purposes as part of a correctly audited process, then that specific media could be considered as the master copy. b) if the media is removed or returned without appropriate auditing, then it constitutes an uncontrolled copy, which could reduce its evidential value.

10 Covert Surveillance Systems

10.1 When-ever possible ACC shall refer situations where covert CCTV cameras are deemed to be required to be necessary to the Grampian Police. However, there are some circumstances were ACC may wish to carry out covert surveillance. When undertaking covert CCTV surveillance operations due regard shall be had to the Corporate Protocol for Covert Surveillance which is available on the Zone. Any officer wishing to undertake a covert surveillance operation must have attended the training sessions prior to undertaking the operation[6].

10.2 In a case where putting up signs would not be appropriate because this may prejudice a specific criminal case, the Council may legitimately chose not to display signs provided that certain conditions are met.. These conditions are:-

a) that a specific criminal activity has been identified;
b) that the CCTV cameras are required in order to obtain evidence of that criminal activity;
c) that the use of signs would prejudice the success of obtaining evidence;

10.3 Any information obtained through the use of covert CCTV cameras must only be used for the purpose of preventing and detecting crime or for the apprehension and prosecution of offenders. The information obtained through the use of covert CCTV cameras shall not be used for any other purpose.

10.4 Prior to undertaking any covert CCTV surveillance the service area concerned must consult with Grampian Police, and the Aberdeen City Council solicitor who is responsible for giving guidance on data protection matters, (or the Information Management Liaison Officer)[7].

10.5 After the above consultation has taken place authorisation to use any covert cameras must be granted in writing by the relevant Head of Service, in accordance with the Corporate Procedure for the Authorisation of Covert Surveillance Operations. Authorisation under the Corporate Procedure for the

[6] For more information on the training, please contact the Head of Legal and Democratic services.
[7] Details of Information Liaison Management Officers can be found on the Zone.

Authorisation of Covert Surveillance Operations may also be required for use of overt CCTV cameras as part of a particular directed covert surveillance operation.

10.6 Authorisation for the use of covert CCTV cameras shall only be given either:
a) after all other possible means of obtaining the necessary evidence of criminal activity have been tried and are deemed to have failed; or
b) The urgency or seriousness of the situation warrants the use of covert CCTV surveillance as soon as possible.

10.7 Covert CCTV monitoring shall not take place for any longer than is necessary.

11 ACQUIRING CCTV SYSTEMS AND MAINTENANCE CONTRACTS

11.1 No CCTV systems or parts of CCTV system equipment whether bought, hired, or leased shall be acquired without first going through the appropriate Council procurement procedures. Decisions regarding the acquisition of such equipment shall be made by appropriate personnel (Council committee or person with delegated authority to make such a decision having regard to the Council's standing orders and financial regulations). As far as possible all CCTV equipment, systems and signs shall be standardised throughout the Council and all systems which are bought, hired or leased shall be capable of being networkable. Such contracts shall refer to this procedure and the standards set out within it, as appropriate.

11.2 Only one CCTV Maintenance Contract shall exist in respect of all Aberdeen City Council's CCTV and alarm systems at any one given time. However this may not include CCTV and alarm maintenance contracts for CCTV and alarm systems in which Aberdeen City Council may be involved as a partner to another organisation, such as Grampian Police. If ACC CCTV and alarm systems are currently tied up in existing maintenance contracts then time will be allowed for these contracts to be fulfilled. However when these contracts are finished every ACC CCTV and alarm system will join the new CCTV and alarm maintenance contract.

11.3 All CCTV/Alarm Control Room contracts in which Aberdeen City Council is involved as a partner organisation shall have a clear service level agreement set out between Aberdeen City Council and its partner organisation. These service level agreements shall set out clearly what is, and what is not required of Aberdeen City Council in respect of the CCTV/alarm equipment.

12 MISUSE OF THE EQUIPMENT AND DISCIPLINE

12.1 Any person found misusing the equipment or the information obtained from any of the recordings whether it be analogue or digital recordings will be considered

to have breached this policy and may have committed an offence in terms of the DPA1998, which is a **personal** liability.

12.2 Any misuse of CCTV systems or of information obtained through either video or CD recording or any other medium will be considered a disciplinary offence and will be dealt with under Aberdeen City Council's agreed disciplinary procedures.

13 COMPLAINTS

13.1 It is the responsibility of ACC to ensure that all complaints are dealt with fairly and appropriately.

13.2 All complaints will be recorded in a complaint log. The complaint log shall detail the number of complaints received, the nature of the complaints received and an outline of the action taken.

13.3 The owners and managers of the CCTV systems shall have a clearly documented complaints procedure. Complaints must be recorded in the complaints log, acknowledged and acted on in an appropriate manner.

13.4 Any person wishing to complain about the operation of the CCTV system should, in the first instance, write to the manager responsible for monitoring the system outlining the nature of the complaint. If the complaint is connected to an occurrence that may have been recorded it is imperative that the manager is contacted within 14 days of the occurrence, as recorded images will not normally beheld beyond that period.

13.5 In the event that any complaint has not reached a satisfactory conclusion in respect of any Data Protection issues, the person making the complaint will be advised to contact:

- The First Contact Team, Information Commissioners office,
  Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
  Tel: 01625 545700
  Fax 01625 524510
  e-mail: casework@ico.gsi.gov.uk

14. AUDIT OF CCTV

14.1. PURPOSE

To carry out an annual assessment/elevation of CCTV to ensure it is 'fit for purpose' and that remedial action is taken for any problems.

14.2. SERVICE STANDARDS

A CCTV Compliance Report will be completed for each site which has CCTV and be returned to the Head of Legal and Democratic Services on an annual basis.

14.3. PEOPLE INVOLVED

The nominated member of staff on site responsible for management, operation, control and maintenance of CCTV.

14.4. METHOD

(a) The equipment will be listed.

(b) A site evaluation of cameras/monitoring equipment will be carried out.

(c) The Systems Manager will confirm if equipment is satisfactory/unsatisfactory, will specify reasons for such (if unsatisfactory) and identify remedial action to be taken.

(d) The Systems Manager will also re-evaluate the purpose of the scheme and state reasons for any amendment of purpose.

(e) The Systems Manager will detail the number of access requests within the previous 12 months and the number of complaints.

APPENDIX 1- STYLE SIGNAGE

Style 1- full description.

"IMAGES ARE BEING MONITORED AND RECORDED FOR THE PURPOSES OF CRIME AND PREVENTION AND PUBLIC SAFETY. THE SCHEME IS CONTROLLED BY ABERDEEN CITY COUNCIL. FOR MORE INFORMATION CONTACT 01224 52 2000".

Style 2– shortened version with Icon

"for the purposes of prevention and detection of crime. The scheme is operated by Aberdeen City Council, please contact 01224 522000".

APPENDIX 2- Checklist for CCTV Installations

Initial Assessment

Have you: - ☐

- Determined who is legally responsible for the installation?
- Assessed the purpose of the installation? Is it the most appropriate way to fulfil the purpose?
- Checked that the existing data protection notification covers this purpose?
- Determined who is responsible for continuing compliance with data protection?
- Assessed whether existing installations still fulfil their intended purpose?
- Has crime detection or prevention been proven?
- Should the camera be re-sited?

Signage

Does the sign :-

- Clearly indicate that you are entering an area covered by an installation?
- Clearly state the purpose of the installation or have the camera symbol?
- Clearly identify the data controller?
- Provide a contact point?

See Appendix 1 for examples of signage

- Are all areas covered by CCTV installations clearly signed?
- Are all private areas blanked from the cameras field of view

Image Quality

- Have you checked whether the quality of the image captured is suitable for the stated purpose?
- Do you check the quality of the images between uses?
    - Clarity of image
    - Accuracy of any dates/times recorded on the images
- Do you clean the storage media between uses rather than over storage media existing images?
- Have you checked whether the camera could be re-sited to provide a better image?
- Have you assessed whether a different type of camera should be installed e.g. infrared?
- Is the installation properly maintained?
    - Who is responsible for ensuring maintenance is carried out?
    - Is a maintenance log kept?

Image Management (Tapes or Digital)

- Have you carried out an assessment of the retention period for images from each installation? (Code of Practise mandates a retention period of 28 days)
- Are procedures in place to record images taken out of rotation e.g. for evidential purposes?
    - Date and time removed
    - Reason for removal
    - Crime reference number (if appropriate)
    - New location
- Is security of the images and recording equipment adequate?
- Have you ensured that images and recording equipment can only be accessed by authorised personnel?
- Have you ensured that monitoring equipment is not on public view?
- Are procedures in place to record viewing of images?
    - Date and time image removed for viewing
    - Name of the person removing the images
    - Details of the person(s) viewing the image
    - Reason for viewing
    - Outcome of viewing
    - Data and time returned to storage

Appendix 3

Form ADM 8/9 (Jan '09)

GRAMPIAN POLICE

Keeping our communities safe

REQUEST FOR THE DISCLOSURE OF PERSONAL DATA TO GRAMPIAN POLICE FROM EXTERNAL ORGANISATIONS Under Sections 28(1), 29(3), Schedules 2, 3 of the Data Protection Act 1998

To:

Name	«name»
Position	«position»
Organisation	«organisation»
Address	«address»

If this request is to be sent by fax, state the number of pages «no» and fax number sent to «to».

I am making enquiries which are concerned with: *Tick as necessary

☐ The prevention or detection of crime*

☐ The prosecution or apprehension of offenders*

☐ Safeguarding National Security*

☐ Protecting the vital interests of the Data Subject or another person*

I confirm that the personal data requested are needed for those purposes and failure to provide the information will, in my view, be likely to prejudice those matters.

Brief details of information required:

«details»

Recipients of this request who subsequently receive Subject Access application for access to this document under Section 7 of the Data Protection Act 1998, are required to consult with the Data Protection Officer at Woodhill House, Westburn Road, Aberdeen, AB16 5AB, before disclosing any information from this document to the applicant.

From:

Rank/Number/Name «rank/no/name»

Station «station» Telephone Number «telno»

I understand that if any information on this form is omitted or wrong, I may be committing an offence under Section 55 of the Act.

Signature _____

Counter Signature _____

Rank/Number/Name «rank/no/name»

NOTES FOR GUIDANCE ON THE COMPLETION OF THE ADM 8/9

The form should be addressed to a specific individual within an organisation.

The Data Protection Act 1998 only allows release of information where both the information is required for one of the purposes listed and failure to disclose the data would be likely to prejudice the matter. This form must not be used where only the purpose is to confirm known facts, for general intelligence, or for administrative reasons.

Organisations to whom this form is sent are not compelled to make the disclosures requested by Grampian Police. Compulsion can only be achieved by Court Order though this is very rarely necessary.

If you require any further guidance on the use of Form ADM 8/9, please contact the Data Protection Section.

Appendix 4

CCTV Annual Compliance Report

Directorate/Head of Service	
Manager	
Date	
CCTV Equipment Sites	**1.** **2.** **3.** **4.** **5.** **6.** **Use other sheet for additions**
Site Evaluation of Cameras/Monitoring Equipment	**Satisfactory ---------** ☐ **Unsatisfactory ------** ☐ **Please specify reason(S) ---------** **Please specify remedial action(s) -------**
Storage media degaussing and disposal conforms to procedure	**Yes ----------** ☐ **No ----------** ☐ **Please specify remedial action(s) -------**
Reevaluate and confirm purpose of scheme **- state reasons for amended purpose**	
Number of access requests within the previous 12 months	
Number of complaints within the previous 12 months	

Signature……Date……..

- APPENDIX 5

CCTV MAINTENANCE REPAIR LOG

Site -										**Site ID-**
Reporting Details						Repair Details				
Maintenance Repair **Emergency**	**Location Camera**	**Details of Fault**	**Reported By**	**Date** *Identified*	**Time**	**Engineer/Company**	**Date** *Info* **Passed**	**Time on** **Site**	**Time off** **Site**	**Action Replace Camera etc**

Appendix 6

Input the information from general storage media log and include date placed in secure area

Manager will confirm if storage media to be returned to stock and not to be released to individual.

CCTV STORAGE MEDIA LOG - REMOVAL

Area	Storage media ID	Date storage media to secure area	Edit/Copy Date out	Edit/Copy Date in	Date Copy storage media released Or returned to stock	Identity of person Removing storage media	Signature
2	**Norfolk - A0002**	**250701**			**250701**	**PC Brown F234**	
4	Norfolk - A0004	300701			020801		
1	Norfolk - A0006	280701	290701	300701	310701	John White Tenant 6 Norfolk Court	

If edit/copy of storage media required, manager will inform senior officer. Police may remove storage media for URGENT matter providing a production form, without obtaining a copy. In general, the storage media will be copied and then passed to the police/individual.

Appendix 7

REQUEST FOR ACCESS TO DATA

DATE	Name/Address of person requesting access	Access Details	Date form issued	Date form returned 40 days to respond	Access authorised / denied (Reason) and date	Date Complete - Storage media issued / access denied
310701	Joe Bloggs, 66 Norfolk Court	CCTV - 250701. Norfolk -A0004 @ 7.05 - 7.15 am	300701 Psmith	010801	Denied - subject not on CCTV at that time. Manager 020801	Storage media back to general use 020801

Manager will record date and name of person requesting access.

Manager will record details of what date, time and area is being requested.
Note that the individual will not know the Storage media ID but they should provide details of whereabouts for staff to determine which storage media will be relevant.

Manager will record date the form was issued - in this example it has already been issued by the CCTV operator who has subsequently notified the Manager to anticipate an Access Request.

Upon receipt of the request and identification of subject verified, the Manager has 40 days to provide the data or deny access.

Record the decision, Manager name and date.

Record that storage media has been returned to CCTV Operators for general reuse.

Appendix 8

Input the time, date and officer changing storage medias. Move the old storage media to a secure place.

CCTV STORAGE MEDIA LOG – GENERAL USAGE AND VIEWING

Area	Storage media ID	Time In	Date	Duty Officer	Date Viewed	Name(s) of viewee(s)	Reason to view	Action taken
1	**Norfolk-A0001**	**12.00**	**250701**	**Psmith**				
2	**Norfolk-A0002**	**12.00**	**250701**	**Psmith**	250701	Psmith PO Name	Police respond to incident	Storage media viewed by Officer F234 and replaced with **Norfolk-A0005**
3	**Norfolk-A0003**	**12.00**	**250701**	**P**				
4	**Norfolk-A0004**	**12.00**	**250701**	**Psmith**	300701	Psmith Authorised HSG staff	Incident reported for time 07.08	Storage media to safe storage noted on Storage media log "Removal" sheet and Access Form issued to JBloggs
2	**Norfolk-A0005**	**02.17**	**250701**	**Psmith**				

Note if a storage media is viewed and a new storage media input, include the reason and the action taken and the date/person. If storage media to be removed, senior officer to complete Storage media log "Removal" sheet- Police should also provide a Production Form.

If at a later date - and within 28 days otherwise the storage media will be cleaned - there is a need to view a previous recording, it should be noted on this form beside the storage media entry. The person viewing the storage media will record their details and why they are viewing, with any subsequent action.

Each CCTV site normally has more than one camera - each site should be coded, e.g.:
Area 1 - Front Door Block 66
Area 2 - Back Door Block 66, etc.
Keep a note of the list easily to hand.

Each storage media should have a reference marked on it at site - suggestion for the reference number is to include the name of the site or similar, followed by a number.