



CCTV CODE OF PRACTICE

Approved by Policy and Governance OCIP Group, 6 November 2009

CONTENTS

1. INTRODUCTION

- 1.1 Legislation
- 1.2 Scope
- 1.3 Responsibilities

2. CCTV IMPACT ASSESSMENTS

3. ADMINISTRATION

- 3.1 Responsibilities
- 3.2 Notification
- 3.3 Data Processing Agreements

4. SYSTEM OPERATION

- 4.1 Image Processing
- 4.2 Overall Responsibility
- 4.3 Audit

5. CHOOSING, PLACING AND USING THE CAMERAS

- 5.1 Siting
- 5.2 Quality of Images
- 5.3 Review and Maintenance
- 5.4 Audio

6. STORAGE

- 6.1 Storage
- 6.2 Placement of Monitors / Viewing Images

7. RESPONSIBILITIES

- 7.1 Signage
- 7.2 Data Protection Requests
- 7.3 Freedom of Information Requests
- 7.4 Other Responsibilities
- 7.5 Other Recorded Information

Appendix 1: Section 29 Form

Appendix 2: Subject Access Request Form

Appendix 3: Sample CCTV Sign

Appendix 4: Maintaining an Audit Trail

1. INTRODUCTION

1.1 Legislation

Information held by organisations about identifiable individuals is covered by the Data Protection Act 1998 (DPA), and this includes the installation and operation of Closed Circuit Television systems (CCTV). This Code of Practice details the manner in which the Council will operate its CCTV systems in compliance with the DPA and any other relevant legislation (including the Human Rights Act 1998).

The Code will be reviewed every three years and, if appropriate, amended to retain its relevance. If at any time there is a need to bring forward changes to reflect statutory requirements or other developments that would be considered beneficial to the Council or the operation of this Code, it will be done within the review period.

Any covert surveillance operations using CCTV will be undertaken in line with Council policy and within the provisions of the Regulation of Investigatory Powers (Scotland) Act 2000. Separate guidance on covert surveillance is available on the Council's intranet, *eric*.

1.2 Scope

The CCTV code of practice applies to all CCTV systems owned by, operated by, or operated on behalf of, Perth and Kinross Council.

It is intended for use by all employees with responsibility for CCTV systems.

1.3 Responsibilities

Each CCTV system must have an identified asset owner who has overall responsibility for the system, its use, the data it records, and the use of that data. This will normally be the relevant Head of Service. The asset owner is responsible for ensuring that the system is appropriately managed and that all employees involved with the system comply with the requirements of this code and the operational procedures contained within it

2. IMPACT ASSESSMENTS

A CCTV impact assessment must be completed at an early stage in the consideration of each new CCTV installation. This should take into account the benefits that can be gained from installing the system, whether better solutions exist, and what effect the new system may have on individuals and their privacy. The impact assessment must be approved by the Council's Data Protection Officer and the asset owner **before** the system is installed.

The impact assessment for every CCTV system must be reviewed annually and approved by both the Data Protection Officer and the asset owner to permit the continued use of the system.

If an impact assessment is not available for a CCTV system, one must be prepared and approved to permit the continued use of the system.

More information on CCTV impact assessments is available from the [Information Commissioner's](#) website or by emailing the Council's Data Protection Officer at dataprotection@pkc.gov.uk.

3. ADMINISTRATION

3.1 Responsibilities

Perth and Kinross Council is the data controller for all the CCTV systems it owns or operates, or are operated on behalf of the Council. Each Service within the Council has responsibility for its own CCTV schemes and the subsequent training and awareness of relevant staff.

3.2 Notification

Perth and Kinross Council must notify the Information Commissioner of how it processes personal data, and review and renew this entry on an annual basis. The notification covers the use of CCTV systems for crime prevention and prosecution of offenders, and specifically covers the:

“operation of CCTV systems in shopping centres, housing estates, schools and other Council premises. Includes the use of Closed-Circuit Television for the monitoring and collection of sound and / or visual images for the purpose of maintaining security of premises, for preventing crime and investigating crime and for administrative purposes and clarification in the event of dispute.”

The Data Protection Officer must be consulted prior to using CCTV for any purpose other than those listed in the notification entry.

The Council's complete notification is available to view on the Information Commissioner's website at:

<http://www.ico.gov.uk/ESDWebPages/DoSearch.asp?reg=4095325>

3.3 Data Processing Agreements

Need clarification on whether any organisations provide data processing services e.g. pixelating (Tayside Police?)

4. SYSTEM OPERATION

All CCTV systems must be operated in accordance with the guidance set out in the Information Commissioner's [CCTV Code of Practice](#).

4.1 Image processing

Images captured on CCTV systems should only be used for the purpose for which they were captured, and should not be used for any purpose other than those notified with the Information Commissioner's Office (see section on 'Notification' for more information)

Rights of access to images are covered in the 'Storing, viewing and disclosing images' and 'Responsibilities' sections of this code.

4.2 Overall responsibility

Responsibility for using a CCTV system in compliance with the code of practice lies primarily with the designated owner, but also with the operators / manager of the system.

4.3 Audit

All CCTV systems may be subject to spot checks to ensure compliance with procedures, including this code of practice and the Information Commissioner's guidance. The Data Protection Officer reserves the right to audit CCTV systems or delegate responsibility for auditing as required.

The ongoing use of a CCTV system may be considered during the auditing process.

5. CHOOSING, PLACING AND USING THE CAMERAS

5.1 Siting

Prior to installing a CCTV system, consideration should be given as to whether or not constant recording is necessary or whether it might only be required during certain time periods. For example, if the objective of the system is to deter night-time burglaries then there should be no requirement to have the cameras recording 24 hours a day.

CCTV cameras must be sited and image capture restricted to ensure that they do not view areas that are not of interest and not intended to be the subject of surveillance (such as an individual's private property).

All cameras must be sited in such a manner that the risk of theft, malicious damage or unlawful tampering is controlled and minimised.

5.2 Quality of images

CCTV systems should have the necessary technical specification to ensure the images are of the appropriate quality. Images produced must be of sufficient size, resolution and frames per second. To make a judgement on the quality of images necessary, the Information Commissioner recommends identifying the needs of a CCTV system by using four categories:

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

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

Recognising: to recognise somebody you know, or determine that somebody is not known to you

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

5.3 Review and maintenance

Having established the quality of images necessary, it is important that a review and maintenance regime is set up to ensure the continued suitability and quality of the system. The recording medium should be set-up in such a way that images cannot be inadvertently corrupted. A regular check should also be made to ensure the date and time stamp on the images is accurate (and amended as required when the clocks go forward / backwards an hour for British Summer Time).

5.4 Audio

CCTV systems must not be used to record conversations or capture sound as a matter of course. Systems should be selected without audio recording if possible, or turned off / disabled in some way if they are equipped for sound. Particular attention must be given to privacy issues if the need to record sound has been identified and the Data Protection Officer should be consulted at an early stage.

6. STORING, VIEWING AND DISCLOSING CCTV IMAGES

6.1 Storage

Recorded material must be stored securely to ensure the integrity of the images and to protect the rights of those whose images may have been recorded. It is possible that the images may be used as evidence in court, so access to the images should be restricted and monitored.

For digital CCTV systems, where the data is recorded and stored on the same device, appropriate provision should be made for backing-up the data and the secure storage of the back-ups.

6.2 Placement of monitors / Viewing images

As far as is reasonably possible, all monitoring and control equipment should be kept away from common view. No unauthorised persons should have access to the control and monitoring areas unless such access is justifiable.

Viewing of live images on monitors should usually be restricted to the operator unless the monitor displays a scene which is also in plain sight from the monitor location. For example:

Pupils in a school can see themselves on a monitor screen. This is acceptable as they cannot see anything on screen which they could not see by looking around them. The only pupils who can see the monitor are those who are also shown on it.

Monitors in a Council office reception area show employees in the corridor and lifts, i.e. out of sight of the reception area. They should be turned so that they are only visible to nominated employees, and members of the public should not be allowed access to the area where operators can view them.

Recorded images should only be viewed in a restricted area, such as a designated secure office. The monitoring or viewing of images from areas where individuals would have an expectation of privacy should be restricted to specifically authorised persons.

If the monitoring/control equipment is to be left unattended it must be secured against unauthorised access or tampering.

In the event of the monitoring/control equipment having to be left unattended in the event of a building evacuation it must be secured against unauthorised access, i.e. the room in which the equipment is housed should be capable of being locked, or alternatively the equipment should be positioned in a lockable cabinet.

6.3 Disclosure of images – law enforcement

Disclosure of images from CCTV systems must be controlled and consistent with the purpose for which the system was established. Requests for access to images may be made by law enforcement agencies such as the Police, but should be accompanied by a signed request form (otherwise known as a 'Section 29 Form' – see Appendix 1). This should clearly state the purpose for which the information is being requested. Details of the request and the information released must be recorded including the reason for the request, the identity of the requestor, the date and time of the recording, and the information disclosed.

6.4 Disclosure of images – individuals

Under the DPA, an individual is entitled to receive access to images of themselves recorded by Council owned / operated CCTV systems, and to be provided with a copy of the images upon request. Requests for access should be made by completing a 'Subject Access Request Form' (see Appendix 2) and follow the Council's subject access request procedures. All requests are subject to a fee of £10 and should be satisfied within 40 calendar days. For more information on subject access requests, contact your Service's data protection representative or email dataprotection@pkc.gov.uk

An individual who requests access to images must provide operators with enough detail (current photograph and how they were dressed as well as location, date and time) to allow them to be identified as the subject of the images and to locate the images on the system.

Where disclosure as part of a subject access request would result in the identification of third parties, these images should be pixelated (blurred) before access can be granted. A record of the access request and the information supplied should be taken.

6.5 Retention

Recorded images should be retained for no longer than necessary. The DPA does not prescribe any specific minimum or maximum retention periods which apply to all systems or footage. Retention periods should be determined by balancing the likely future value of the images against the rights of individuals to ensure their images are not held indefinitely.

The Council's current recommended retention periods are 7 days for school recordings, 14 days for car parks, and 31 days for all other systems.

7. RESPONSIBILITIES

7.1 Signage

The Council is obliged to let people know that they are in an area where CCTV surveillance is being carried out. Appropriate signage should be placed in a prominent position at the main entrance points to the areas covered by the CCTV system. Signs should be clearly visible and readable, at an appropriate height, and should indicate the presence of CCTV monitoring, ownership of the system, the objectives / purpose of the monitoring and contact details for more information. Signs should also be an appropriate size depending on context, for example whether they are viewed by pedestrians or car drivers.

Appendix 3 shows an example of the type of information that should be contained on a sign.

7.2 Data Protection requests

Requests made by individuals for access to CCTV images in which they are recorded should be treated as subject access requests under the DPA. See section on '*Disclosure of images – individuals*' for more information.

7.3 Freedom of Information requests

As a public authority subject to the Freedom of Information (Scotland) Act 2002 ("FOISA"), the Council may receive a request for CCTV footage under this Act.

Freedom of Information requests should be directed to, and processed by the Council's Freedom of Information Team. Requests should be satisfied within the statutory 20 working days limit. For more information email foi@pkc.gov.uk

Section 38 of FOISA contains an exemption for personal information. Requests for images of the requestor should be treated as a subject access request under the DPA. Requests for images of other people are likely to be subject to the section 38 exemption and are unlikely to be disclosed.

All FOISA requests will be processed on a case-by-case basis.

7.4 Other responsibilities

The Information Commissioner has advised that – whilst unlikely to receive such requests - employees operating the CCTV system should be aware of two further rights that individuals have under the DPA. These are:

- *DPA Section 10* – an individual's right to prevent processing likely to cause substantial and unwarranted damage and distress
- *DPA Section 12* – a right to prevent automated decision-taking in relation to the individual

For more information on these exemptions please email dataprotection@pkc.gov.uk

7.5 Other recorded information

Appendix 4 provides a summary of areas or instances that may be considered useful to record to allow for a clear audit trail. This includes non-routine access to footage, requests for copies or prints, and system faults.

Appendix 1: Section 29 Form



To:
.....
.....

DATA PROTECTION ACT 1998, SECTION 29(3)

I am making enquiries which are concerned with:

- * (a) the prevention or detection of crime
- * (b) the apprehension or prosecution of offenders

Nature of enquiry:

.....

The information sought is needed to:

.....

.....

.....

.....

.....

I confirm that the personal data requested is required for that / those purpose*(s) and failure to provide the information will, in my view, be likely to prejudice that / those purpose*(s).

Signed:

Rank:

Name:
(Block Capitals)

Date:

Police Station:

Countersigned:
(Where Necessary)

Rank:

* *Delete as appropriate*



Data Protection Act 1998

Subject Access Request Form

1. Personal details (Please print clearly in black pen)

Surname _____ Date of Birth _____

Forename(s) _____

Address _____

Post code _____ Tel no (incl. STD code) _____

2. Details of request

Which Perth & Kinross Council Services do you wish to obtain information from ? (please see over for details)

<i>Service</i>	<i>In connection with.....</i>
_____	_____
_____	_____
_____	_____

3. Additional Information

4. Checklist - have you provided

Fee Unless this is an Education only request*, please enclose a fee of £10**. Cheques should be made payable to 'Perth and Kinross Council'.

Proof of Identity (at least one of the following must be brought to your local office):

Passport Birth certificate Driving Licence

* Fees for an Education subject access request are dependant on the number of photocopies required and will be charged prior to the release of any documents.
** If you are unable to pay the fee, please provide details above in section 3.

5. Article 10 Notice

The information provided by you will be used only in processing your subject access request. In terms of the Data Protection Act 1998, you are entitled to know what personal information Perth and Kinross Council hold about you, on payment of a fee of £10. The Council accepts no liability for any documents which you may send to the Council for verification of identity.

Signed _____ **Date** _____

You may ask your Solicitor, Councillor, MP, MSP or MEP to assist in processing your request. You may be required to give written authorisation for them to act on your behalf.

6. Authorisation

I hereby authorise _____ Councillor/MP/MSP/MEP to act on my behalf in relation to this Subject Access request and sanction their access to my personal data.

Signed _____ **Date** _____

About Council services.....

The Council Leaflet 'Access to your personal information' provides details on how to use the Data Protection Act 1998 to gain access to the information which the Council holds about you.

In order for us to locate the information you require, we need to know which services you are interested in. In order to help you identify these services, we have provided a list of those most commonly used which should assist in completing section 2 overleaf.

Service Name	What services might you have received ?	
Financial Services	Council Tax Poll Tax	
Social Work	Advice on benefits Home helps Residential homes	
Housing	Benefit Claims Housing Waiting List Rent Payment	
Education & Children's Services	Pupil records School boards Special Educational Needs	Foster Care/Adoption Childcare Looked After/Accommodated Children
Planning and Development	Planning Applications Building Control	
Roads, Transport & Architectural	Public Transport	
Environment	Outdoor Services Environmental Health Food Safety Health and Safety Enforcement Environmental Services (Refuse Collection, Street Cleaning etc.) Crematorium Burials	
Sport and Culture	Libraries Museums Sports development	
Corporate Services	Personnel Public Relations Committee Services Property	

This list is not exhaustive and should you require any assistance in finding out exactly which service of the Council is concerned with your request, please ask for advice when returning this form.

Appendix 3: Sample CCTV Sign

CCTV IN OPERATION



Data Protection Act 1998

This CCTV system is operated for the purposes of public safety, security of the premises and crime prevention.

This system is owned, operated and registered by Perth & Kinross Council.
(Data Controller).

Perth Academy, Murray Place, Perth

Tel : (01738) 623491



Appendix 4 – Maintaining an Audit Trail

* Please note: the details below are suggestions only, and it is at the discretion of each operator as to what is recorded and maintained and how this is done.

Confidentiality undertaking *(for those viewing images who do not normally have access as a matter of routine)*

A signed undertaking would ensure individuals agree not to alter, destroy or copy recorded data, nor to disclose or distribute any information about the images to a third party without consent of the asset owner.

Incident logging *(where the system has captured an image which requires further action)*

This may cover the date and time of the incident, a brief description of the incident, and a summary of any action required or taken.

Fault logging *(where the system is not recording or operating as intended)*

This may describe the date and nature of the fault, details of when it was reported (and to whom), and the result / outcome of any action taken to fix the fault.

Copies of recordings *(where the footage is required to be copied as a result of a request or incident)*

This would describe the date the copy was made, the date and time of the incident (if applicable), the reason for making a copy, and details of who the images were copied to.

Image prints *(where a still photograph is required, as opposed to real time video footage)*

This should be similar to the information detailed for copies of recordings.