Gwybodaeth
Dan
Reolaeth

Gwynedd Council

Guidance on the use of closed circuit television systems and other surveillance cameras

September 2015

Information Management Service

CYNGOR GWYNEDD COUNCIL

INTRODUCTION

The use of Closed Circuit Television (CCTV) involves the processing of personal data and is therefore subject to the Data Protection Act 1998. As such, the data protection principles must be observed, as well as the Information Commissioner's A data protection code of practice for surveillance cameras and personal information.

The purpose of this document is to provide guidance to staff responsible for CCTV systems and to ensure that they adhere to good practice.

The guidance does NOT apply to:

- Surveillance activities which are carried out under the Regulation of Investigatory Powers Act 2000 (RIPA) – see *Appendix 1*.
- The use of hidden cameras to monitor staff.

1.1 DATA PROTECTION ACT 1998

Since surveillance systems monitor and records the activities of individuals, they process personal information and therefore need to comply with Data Protection legislation. The eight principles are as follows:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate and kept up to date;
- Not kept for longer than is necessary;
- Processed in accordance with individuals' rights;
- Secure;
- Not transferred to countries without adequate protection

1.2 BEFORE YOU START – Assessing the need for CCTV

Since using CCTV can be privacy intrusive, you should carefully consider whether to use it or whether other solutions can achieve the same objectives.This is done by conducting a privacy impact assessment which takes into consideration data protection and also human rights.

Any assessment of a system should consider the following:

- What are the benefits to be gained from its use
- The purpose of the system e.g. crime prevention, security of property, staff and/or public safety.
- Could other methods be used e.g. improved lighting?

If you decide, based on the assessment above, that you need to install CCTV, then ensure that you adhere to the following good practice.

PRACTICAL GUIDANCE

1. RESPONSIBILITIES

Gwynedd Council is the data controller for the Council's CCTV systems. This means that it is the Council that registers the use with the Information Commissioner, and decides how the images should be used and to whom they may be disclosed.

However, each individual system should have an 'owner' who is responsible for its day to day operation.

1.1 Establish and identify the person in the service who is responsible for operating the CCTV system on a day to day basis.
1.2 He/she should be responsible for ensuring that the operators understand the purpose of the system.
1.3. He/she should be responsible for ensuring that procedures and standards are being complied with and that the system complies with this guidance.

2. USING THE EQUIPMENT

2.1 Siting and use of cameras

The equipment must be adequate for the purpose. Cameras should be sited in appropriate locations and should not view areas that are not of interest e.g. private property.

2.1.1 Use the cameras only to view space(s) which are relevant.
2.1.2 Ensure that you **only** use the cameras for the purposes of your scheme.
2.1.3 Consider whether the cameras are of the right size for the location and are of the necessary technical specification.
2.1.4 Ensure that the cameras are in a secure location and not easily damaged.

2.2 Maintenance of system and recording equipment

It is important that the CCTV system can produce images of the appropriate quality.

2.2.1. Check the operation of the CCTV system on a regular basis
2.2.2. If the system records the date and time, these should be accurate
2.2.3. Cameras should be serviced and protected from vandalism
2.2.4. A detailed maintenance log should be kept

2.3 Storing and viewing

Recorded material should be stored in a way that maintains the integrity of the image to ensure that the rights of individuals recorded by the system are protected and that the material can be used as evidence in court, if necessary.

You therefore need to choose carefully the medium on which the images are stored and then ensure that access is restricted.

2.3.1 Only staff who need to use the system to achieve the purpose should have access to recorded material

2.3.2 Recorded images should be viewed in a restricted area, e.g office of the manager or designated member of staff. Access to others should be denied when images are being viewed.
2.3.3 The monitor viewing area should be appropriate.
2.3.4 Access to this area should be limited to those persons who have a real need to be there.
2.3.5 Information should be kept secure.
2.3.6 Staff should be made aware that misuse of the equipment may constitute an offence.

2.4 Method of transferring footage to third parties

2.4.1 You should ensure that recorded material can be easily transferred to the police and others, especially if using digital recording technology.
2.4.2. You should ensure that it can be provided in a suitable format without losing image quality.
2.4.3. A secure method of transfer should be used.

The form in *Appendix 2* outlines the procedure to be followed.

2.5 Retention of images

The retention period for images should reflect the purpose of the system and should not be kept for longer than necessary. When there is a criminal investigation images will need to be kept for longer – the original must be retained for 7 years.

2.5.1 You should ensure that staff know the retention period for the images. The Council's policy is to retain images for 30 days when there is no criminal investigation.
2.5.2 Images should be securely deleted at the end of this period.
2.5.3 A record or audit trail of the deletion process should be maintained.

2.6 Quality of images

2.6.1. The system should produce good clear quality information.
2.6.2 The date and time stamp used should be accurate.
2.6.3 Any wireless transmission system used should be secure.

2.7. Audio recording

Systems should not normally be used to record conversations between members of the public as this is highly intrusive.

2.7.1. A system without this facility should be chosen where possible or if not, be turned off unless there is particular justification for retaining it.
2.7.2 Audio recording should only be used where there is a pressing social need and you have reviewed other less privacy intrusive methods.

2.8 Signs

You must let people know that they are in area where CCTV is being used.

2.8.1 The presence of CCTV must be publicised by using prominent signs of an appropriate size

2.8.2 Signs must specify the name of the service or who is operating the CCTV, the purpose of the system and contact details of the organisation responsible.

2.8.3. If audio recording is taking place, this should be made clear to the individuals involved.

3. BODY WORN VIDEO (BWV)

3.1 It is important to know when and when not to record. Continuous recording can be excessive especially if is going to capture bystanders. For example, it may be appropriate for a parking enforcement officer to switch on their BWV camera if they believe an individual is going to be aggressive.

3.2 Consideration should be given to using systems where video and audio recording can be controlled and turned on and off independently of each other.

3.3. It is important that clear signage is displayed, for example, on an individual's uniform, to show that recording is taking place and whether the recording includes audio.

3.4 Since sensitive information may be captured by BWVs, the devices must be kept secure e.g. by encryption.

3.5 Processes should be in place to specify how long the information should be kept and then that it is securely destroyed at the end of the period.

3.6 Recordings should be stored so that specific events can be easily retrieved.

4. SUBJECT ACCESS REQUESTS

Section 7 of the Data Protection Act gives individuals the right to access personal information. Therefore, individuals whose images are recorded have a right to view and to be provided with a copy of the images.

4.1 There is a form available for this purpose (see *Appendix 3*)

4.2 The Council must respond within 40 calendar days and a fee of £10 will be charged.

4.3. Images of third parties may also have been recorded - you will have to decide, in accordance with the circumstances, whether or not their faces will need to be obscured.

4.4. If an external company is being used to edit images, there should be a written contract between the Council and the company.

5 FREEDOM OF INFORMATION ACT REQUESTS

5.1 Any freedom of information requests for CCTV images should be referred to the Information Manager who will respond to them in accordance with the provisions of the Act.

6. DISCLOSURE OF INFORMATION TO THIRD PARTIES

Disclosure of images to third parties must be consistent with the purpose for which the system was established e.g. if the purpose is to prevent and detect crime it will be appropriate to disclose to the police but not to the media.

Any other requests for images should be approached with care.

6.1 Disclosure to third parties will only be permitted under certain circumstances e.g. if the purpose is to prevent and detect crime, access should only be granted to:

- Law enforcement agencies
- Prosecuting bodies
- Legal representatives

- Individuals who appear on the footage (unless this would prejudice legal proceedings)

6.2. All requests for viewings must be recorded

- Record the date and time
- Why the images are being viewed
- Who is viewing the images
- If the request has been made by the police, they should fill in a form which has been authorised by an inspector or senior officer. Contact the Information Manager to obtain a copy of the form.

7. COMPLAINTS AND MISUSE

7.1 Any complaints made by the public about the CCTV system will be dealt with under the Council's complaints procedure and/or Social Services complaints procedure, as required.

7.2. Misuse of the CCTV system by a member of staff will be dealt with under the Council's disciplinary procedure. Misuse of the system can be a criminal offence.

8. MONITORING THE OPERATION OF THE SYSTEM

8.1 The number of complaints received should be recorded.

8.2 The effectiveness of the system should be assessed by an annual internal review.

8.3 The results of the assessment should be considered in light of the purpose of the system. If it does not achieve its purpose, its operation should cease.

Appendix 1

Regulation of Investigatory Powers Act 2000

The Council has a separate policy on this Act - Corporate Policy and Procedures Document on RIPA 2000.
If CCTV is used for the purposes of the Act, this use must be authorised via a directed surveillance authorisation which must

i) Specify what activity is being authorised
ii) Explain how this will be done (which cameras will be used)
iii) Set out which activities will be recorded.

The member of staff responsible for the CCTV system must ensure that they understand the conditions of the authorisation. The relevant sections of the policy are reproduced below:

"8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others. The Council has a specific Policy on the use of CCTV cameras and images. However, the operation of that Policy **does not** override the need to comply with the requirements of this *RIPA* Policy."

" When some other agency (e.g. Police, Customs & Excise, Inland Revenue etc):-

(a) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Head of Administration and Public Protection for the Central Register) and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources;"

Record of Evidence Disclosure - Closed Circuit Television (CCTV) Footage

The purpose of this document is to record the instances of evidence disclosure to law enforcement agencies where Gwynedd Council is the data controller as designated within the Data Protection Act 1998.
This form is to be retained by Gwynedd Council and serves as a log of the evidence disclosure process.

THIS RECORD MUST BE RETAINED FOR <u>SEVEN YEARS</u> FOLLOWING DISCLOSURE (expiry date [+7]:……..)

Details of request: *(reference, requester(s), recipient(s), date, description)*

Particulars of information request: *(dates and times of footage, camera name / area filmed)*

CCTV System Details: *(suppliers, hardware, software, data retention period and any other relevant particulars)*

Pre-download Integrity Verification: *(Is CCTV date and time correct? note any discrepancy from GMT/GMT+1 and any amendments necessary to fulfil evidence request)*

Data Collection Notes: *(date, time and process)*

(details of Gwynedd Council staff or agents conducting the download)

Name……..……..……..
Post……..……..……..……Signature…….……

Name……..……..……..
Post……..……..……..……Signature…….……

Name……..……..……..
Post……..……..……..……Signature…….……

(Details of any additional individuals present in location/room and purpose of presence)

Data Storage:
(describe media used to store footage, describe fully any instances of copying the files - including the hardware used and its owners - as part of the evidence disclosure process).

***(if evidence is stored prior to being disclosed**, note location and access controls – is location locked?, who has access?, is there a log of visitors to site? – note all movements of evidence prior to disclosure including personnel involved and purpose of movement)*

(use additional space over if required)

Record actions taken following download and prior to disclosure, e.g. details of contact with law enforcement agency to arrange disclosure – record dates, times, personnel involved and any action plans agreed.

Responsibility for possession of the evidence prior to disclosure:

Name:……..……..…… Post……..…
Signature…….

Turn over for disclosure record

Disclosure Record:
Date and location of disclosure of evidence:

Disclosed by (on behalf of Gwynedd Council):

Name:……..….Post:…… ……..

Contact Details:……..

Signature…… Date…….

Disclosed to:

Name:…..…….Post/Position:…… ……

Organisation:……..
Contact Details:…….

Signature…… Date…….

At the point of disclosure, responsibility for handling the evidence is accepted by the recipient organisation represented by the above signatory. Gwynedd Council accepts no liability for the admissibility of the evidence following this disclosure. Recipients are advised to contact Gwynedd Council promptly if any issues arise concerning the quality or integrity of the evidence as a reproduction of the evidence will not be possible when the source is overwritten.

Record of change or movement of evidence prior to disclosure

Use this space as additional space to record any changes to the status of the evidence following the download and prior to disclosure.

- Record any movement between locations in a room, movements between rooms, and movement between sites – record dates and times, a full description of the purpose of the movement and record the access control of all the locations involved, e.g. is it locked?, who has access?, is there a log of access?.
- Record any changes to access control details, e.g. changes to key holders of storage location.
- Record any instances of copying data from the master copy of the evidence.

Date and time [] Details of change [] Purpose of change [] Personnel Involved [] Signatures [] Access Control Details

Additional Notes: *Include date and signature if relevant*

THIS RECORD MUST BE RETAINED FOR SEVEN YEARS FOLLOWING DISCLOSURE

Data Protection Act 1998
Subject access request – CCTV systems

This application form is used to allow individuals access to information held about them on Gwynedd Council's CCTV system. **If you have not already done so please enclose a cheque or postal order for £10 made payable to Gwynedd Council.** The Data Protection Act allows a charge of up to £10 to be made to process an application.

Gwynedd Council reserves the right to verify the identity of the individual making the request. Under the provisions of the Act Gwynedd Council must respond within 40 days to the request. If Gwynedd Council or the individual require further information e.g. proof of identity, the 40 days will recommence from the time the information is received. You will be notified in writing when your application is received.

Section 1 – Personal Details

Name	
Surname	
Date of birth	
Address	
Post Code	
Telephone	

Section 2 Proof of identity

To help establish your identity your application must be accompanied by official documents. For example: copy of birth certificate, driving licence, recent original utility bill.

Also a recent full face photograph of yourself.

Failure to provide this proof of identity may delay your application.

Section 3 Supply of Information

You have the right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:

(a) View the information and receive a permanent copy Yes/No

(b) View the information only Yes/No

Section 4 – Declaration

The information that I have supplied in this application is correct and I am the person to whom it relates **Signed** **Date**

Section 5 – To Help us Find the Information

If the information you have requested refers to a specific offence or incident, please complete this Section.
If the information you require relates to a vehicle, property or other type of information, please note below.

Were you: (tick box below)	
A person reporting an offence or incident	☐
A witness to an offence or incident	☐
A victim of an offence	☐
A person accused or convicted of an offence	☐
Other – please explain	

Date and time of incident	
Place of incident	
Brief details of incident	

Before returning this form please check: **Have you completed ALL sections?** **Have you enclosed the identification documents?** **Have you signed and dated the form?** **Have you enclosed the fee?**

Please send this form to the Information Manager, Information Management Service, Gwynedd Council, Caernarfon, Gwynedd. LL55 1SH