Northumberland
County Council

CCTV POLICY

DOCUMENT REFERENCE	VERSION	DATE OF THIS VERSION	DATE OF ORIGIN
NCC/IG03	3.5	18/02/2016	08/10/2008

	APPROVED BY	APPROVAL DATE
1	Data Protection Officer	24/05/2018

DATE REVIEWED	REVIEWED BY	APPROVAL DATE	NEXT REVIEW DATE
February 2016	Data Protection and Information Governance Officer		May 2020

.

Northumberland
County Council

Related Policies

POLICY NAME	POLICY REFERENCE NUMBER	VERSION
Data Protection and Confidentiality Policy	NCC.IG02	5.3
Freedom of Information Policy	NCC.IG04	2.2
Environmental Information Request Policy	NCC.IG05	1.0
Information Security, Transportation and Sharing of Data Policy	NCC.IG10	
Employee and Elected Members Codes of Conduct		

Amendment History

VERSION	DATE	DESCRIPTION
0.3	15/02/2006	REvised Working Draft
1.0	20/03/2006	Issued
1.1	21/04/2008	Working Draft - rewrite following new ICO Code of Practice 2008
2.0	15/05/2008	Issued
3.0	01/02/2012	Minor amendments
3.1	17/04/2014	Changes to Protective Marking
3.2	22/04/2014	Revised including amendments to section 1, 3, 12, 13, 14 and Appendix 2 and 3
3.3	22/04/2014	Minor amendments following advice from Legal Services
3.4	18/02/2016	Policy put into new format
3.5	18/05/2018	Update to reflect General Data Protection Regulation (GDPR) 2018

.

Northumberland
County Council

Table of Contents

.

Northumberland
County Council

1. Scope

1.1 The scope of this Policy applies to all Northumberland County Council employees and members. Agency workers, partner agencies contractors and vendors who are required to use Northumberland County Councils information systems will also be made aware of and be expected to abide by this policy.

1.2 This policy and supporting guidance confirms how the authority manages its CCTV systems(s), determines who has access to the CCTV data and under what circumstances, including the procedures that will be followed in regard to providing access to CCTV Data.

1.3 This document must be read in conjunction with the Information Commissioner's "CCTV Code of Practice" (Revised Edition) 2008, the Surveillance Camera Code of Practice issued by the Secretary of State pursuant to Section 30 of the Protection of Freedoms Act 2012 and the Northumberland County Council Data Protection Policy, all of which are accessible via the following links.

http://portal.northumberland.local/sites/Policies/Pages/default.aspx

http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

2. Purpose

2.1 This Policy identifies the procedures and processes to be followed when planning, implementing and operating a CCTV scheme on Council premises, and is compliant with the Information Commissioner's Office CCTV Code of Practice (Revised Edition) 2008, the General Data Protection Regulation (GDPR) 2018, and the Surveillance Camera Code of Practice issued by the Secretary of State pursuant to Section 30 of the Protection of Freedoms Act 2012.

2.2 This policy is part of a suite of Information Governance policies.

3. Introduction

3.1 Closed Circuit Television (CCTV) can be a valuable resource in surveillance and security and is widely used by local authorities in a range of premises and situations. However, because of the potentially sensitive nature of surveillance, there are codes, guidelines and

legislation which must be complied with in order to operate a CCTV scheme legally and fairly.

3.2 Images recorded by a CCTV scheme are deemed to be personal data under the terms of the General Data Protection Regulation (2018). The GDPR applies to **'personal data', meaning** any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

3.3 Personal data is not therefore limited to the ability to name an individual. If images of an individual's features are processed and an individual can then be identified from those images, they will amount to Personal Data.

3.4 Data is considered to have been processed from the point at which it is recorded and retained, even if the data is not subsequently viewed by anyone.

3.5 As with other data, the recorded images from a CCTV scheme may be requested by members of the public in the form of a Subject Access Request within the terms of the General Data Protection Regulation.

3.6 It is important that this Policy is read by those considering the installation of a CCTV scheme, and that its contents are complied with following implementation.

3.7 All enquiries about and proposals for CCTV installations must in the first instance be directed to the Data Protection Officer.

4. Legislation

4.1 Any CCTV Scheme owned and operated by Northumberland County Council must comply with the following legislation:

- The General Data Protection Regulation 2018;
- The Human Rights Act 1998;
- The Protection of Freedoms Act 2012;
- The Freedom of Information Act 2000;
- The Regulatory and Investigatory Powers Act 2000

4.2 In addition, the Council is duty bound to have regard to the following statutory Codes of Practice

- The CCTV Code of Practice (Revised edition 2017 - version 1.2) published by the Information Commissioner's Office

- The Surveillance Camera Code of Practice issued by the Secretary of State under Section 30 of the Protection of Freedoms Act 2012

5. Responsibilities

5.1 All CCTV schemes that process Personal Data as defined by the General Data Protection Regulation 2018 require a "Data Controller" to ensure the correct management of the scheme and the processing of recorded images. Where a CCTV scheme is run by a business or organisation such as the Council, it is the "body" that is the Data Controller rather than an individual member of staff. It is nevertheless important at the very outset to establish who will be responsible on site for all aspects of managing the proposed CCTV scheme on site, to ensure the Council complies with legislation and the statutory Codes of Practice.

5.2 If the day-to-day running of the scheme is devolved to someone else, the Data Controller still retains ultimate responsibility for the scheme. The person to whom the running of the scheme is devolved would be committing a criminal offence if s/he were to act outside the instructions of the Data Controller.

5.3 If the scheme is devolved to a third party such as a security company, the advice of the Data Protection Officer must be sought.

5.4 Where two organisations share a scheme, such as a live feed from one scheme to another, and both make decisions regarding its purpose and operation, then they both share responsibility.

5.5 The person responsible for the management of the scheme has a number of responsibilities outlined in this policy. Among these is the need to regularly carry out pro-active checks to ensure that this policy is being complied with, including a review of the on-going value and benefit of the scheme. If the scheme is not achieving its purpose it should be discontinued or modified.

5.6 A public space surveillance (CCTV) licence is required if CCTV is run by operators supplied under a contract for services. It is a criminal offence for staff to be contracted as public space surveillance (CCTV) operators without a Security Industry Authority (SIA) licence.

6. Point of Contact

6.1 There must be a point of contact for members of the public, which will be identified on signage in the area/s covered by the CCTV camera/s. The point of contact must be available

to the public during office hours. All employees at the point of contact must be conversant with Northumberland County Council 'policies and procedures governing Data Protection and the use of CCTV equipment

6.2 Enquirers to the point of contact must be provided on request with one or more of the following:

- This policy
- A subject access request form if required
- Information about the corporate Complaints Procedure if they have concerns about the use of the system or about non-compliance with the Code of Practice and/or this policy.

6.3 A record of the number and nature of complaints and enquiries must be maintained together with an outline of the action taken in response. A report of these figures must be produced regularly in order to assess public reaction to and opinion of the scheme.

7. Establishing the Need for a CCTV Scheme

7.1 While there is a high level of public support for CCTV schemes, there are increasing concerns about the role of CCTV in a "surveillance society". In order to maintain public support and trust, it is important to ensure that the CCTV scheme:

- Is established on a proper legal basis and operated in accordance with the law
- Is necessary to address a pressing need, such as public safety, crime prevention or national security
- Is justified in the circumstances
- Is proportionate to the problem that it is designed to address

7.2 A Data Protection Impact Assessment (DPIA) may be required to determine whether the use of CCTV is justified. An assessment should consider the following:

- What is the purpose for using CCTV?
- What are the problems it is meant to address?
- What are the benefits to be gained from its use?
- Can CCTV technology realistically deliver these benefits?
- Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Are images of identifiable individuals required, or could the scheme use other images not capable of identifying individuals?
- Could more privacy-friendly options be used instead, such as only recording events likely to cause concern, such as movement in a defined area?

.

- Will the scheme 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 they be addressed?
- What are the views of those who will be under surveillance?
- What could be done to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?

7.3 The Information Commissioner's Office has published a 'Conducting Data Protection Impact Assessments (DPIA) code of practice' which explains what DPIAs are and how they can be used to identify and reduce privacy risks associated with projects such as CCTV surveillance.

7.4 The code of practice is accessible via the ICO website. www.ico.org.uk

7.5 A template to record a DPIA is available from the Information Governance Team via Informationgovernance@northumberland.gov.uk. The team can also provide advice, support and guidance on the completion of a DPIA.

8. Establishing the Purpose of a CCTV Scheme

8.1 There are four categories for identifying the purpose for CCTV cameras:

- **Monitoring:** to watch the flow of traffic or the movement of people where it is not necessary 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 who is known, or to determine that somebody is NOT known
- **Identifying:** to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

8.2 The image quality required for each of these purposes varies – further information on this and assistance in selecting equipment is available from the Home Office Scientific Development Branch at nationalarchives.gov.uk

8.3 It should also be noted that if the equipment used records sound, this must not be used to record conversations between other people, although there are some limited circumstances in which audio recording may be justified, subject to sufficient safeguards. Advice on this

can be sought from the Data Protection Officer via informationgovernance@northumberland.gov.uk

8.4 The purpose of the CCTV scheme must be identified and documented, and also the reasons why CCTV is the most appropriate means of meeting the scheme's objectives.

8.5 CCTV schemes can be employed for the following purposes:

- Prevention, investigation and/or detection of crime
- Apprehension and/or prosecution of offenders
- Public and employee safety
- Staff discipline
- Traffic flow monitoring

8.6 Once the purpose of the scheme has been identified it is necessary to:

- Ensure that everyone associated with the scheme is fully aware of its declared purpose, and the privacy implications of its use.
- Ensure that the equipment is only used to achieve the declared purpose
- Decide whether constant real time recording is required or whether specific time periods may be more appropriate.

9 Location of the Cameras

9.1 The location of the CCTV equipment is very important and must be planned carefully. The physical spaces to be covered must be clearly identified, and the way in which images are recorded must comply with Data Protection Principles as follows:

- Cameras must only monitor those spaces intended to be covered.
- Cameras must be situated to ensure that they will effectively capture images relevant to the scheme's purpose.
- If there is a risk of neighbouring spaces being monitored unintentionally the owner of such spaces must be consulted.
- Adjustable cameras must be restricted to prevent operators from being able to allow unintended spaces to be overlooked and/or recorded.
- Cameras must be able to produce images of sufficient size, resolution and frames-per-second
- Physical conditions and environment must be borne in mind when siting cameras, for instance taking into account lighting and the size of the area to be viewed.
- All necessary steps must be taken to protect the cameras from vandalism and theft.

9.2 It should also be noted that some areas have heightened expectations of privacy, such as changing rooms and toilets, and cameras must only be used in most exceptional circumstances to address very serious concerns.

10. Signage

10.1 In order to comply with the General Data Protection Regulation, areas covered by CCTV schemes must display signs warning members of the public. The wording and location of signage must take into account the following points:

- Signs must clearly identify to the public when they are entering an area covered by CCTV. These signs can be supplemented with further signs inside the area of required.
- Signs must be clear and legible both in terms of lettering and size, appropriate to the sign's location.
- Signs must identify:
    - Who is responsible for the scheme
    - The scheme's purpose
    - Details of who to contact about the scheme.
- In exceptional circumstances it may be agreed that signage may compromise the purpose of the scheme. In such cases the owner of the scheme must consult with the Data Protection Officer and Legal Services, and must identify and document:
    - A specific criminal activity
    - The need for CCTV to obtain evidence of that criminal activity
    - The reasons why signage would prejudice success in obtaining such evidence.
    - How long the monitoring should take place to ensure it is not carried out for longer than necessary.

10.2 Where public announcements are already used, the message can be backed up with audio announcements

11. Equipment Quality

11.1 Procedures and systems must be established to ensure that CCTV equipment is adequately maintained and that the quality of images recorded consistently meets the purpose of the scheme.

- Any tapes or other media used must be of good quality and must be cleaned so that images are not recorded over previously recorded images.

.

- Recorded pictures and prints as well as live screens must produce good quality images, and the quality must be regularly monitored.
- If the system records information such as date, time and camera location, this data must be accurate at all times.
- Equipment must be capable of being set up in such a way as to avoid inadvertent corruption
- If an automatic facial recognition system is used to match images, those images must be of a sufficiently high quality to ensure accurate matching. All matches must in any case be verified and documented by a human operator.
- Selection of equipment must ensure that copies of a recording can be made easily if asked for by a law enforcement agency, and their use of the images should be straightforward.
- A maintenance log must be maintained for all equipment associated with the scheme.
- If a camera is damaged, there must be clear procedures for:

    - Defining who is responsible for ensuring repair/replacement
    - Ensuring the camera is repaired/replaced within a specific time period
    - Ensuring the monitoring and documentation of maintenance work.

12. Data Storage and Access

12.1 Retention periods must be established for required and non-required images, and secure and controlled storage and access arrangements for images in compliance with the principles of Data Protection. These must be discussed with the Data Protection Officer, and must take into account the following points:

- Non-required images must be erased as soon as practicable, being permanently deleted through secure methods.
- Required images must be retained for a length of time appropriate to their purpose and the purpose of the scheme.
- Systematic checks must be carried out to ensure compliance with the agreed retention period.
- When the documented period of retention has been reached images must be removed / erased.
- Any images that are to be retained as evidence must be kept in a secure location with controlled access.
- When images are removed for use in legal proceedings the following information must be logged:
- Date on which images were removed.
- The reason why they were removed.
- Any relevant crime incident number.
- The location of the images.

.

- Signature of the collecting police officer if appropriate.
- Monitors displaying images from areas where people would expect privacy must only be capable of being viewed by authorised employees of the User.
- Access to recorded images must be restricted to the designated member of staff responsible for the scheme who will decide whether to allow disclosure to third parties in accordance with the scheme's disclosures policy.
- Viewing of recorded images must take place in a restricted area with controlled access.

12.2 When images are removed for viewing purposes the following information must be logged:

- Date and time of removal.
- Name of person removing the images.
- Name/s of the person/s viewing the images. If this includes third parties it must also include the third party's organisation.
- The reason for the viewing.
- The outcome, if any, of the viewing.
- The date and time images were returned to the system or to a secure area.
- All operators and others with access to images must be aware of the access procedures that are in place.

13. Disclosure of Images

13.1 The designated Manager of the CCTV system must ensure that access to, and disclosure of images recorded by the CCTV system is restricted and carefully controlled.

13.2 The designated Manager must ensure all employees are aware of the following disclosure and access restrictions:

- Access to recorded images must be restricted to those who need to have access to achieve the purpose of the CCTV scheme.
- All access to images must be logged and documented.
- Disclosure of recorded images to third parties must only be made in limited and prescribed circumstances.
- All requests for access or disclosure must be recorded. If access or disclosure is denied the reason must be documented.
- If access or disclosure of images is allowed then the following information must be logged:
    - The date and time at which access was allowed or the date on which disclosure was made
    - The reason for allowing access or disclosure

- The extent of the information to which access was allowed or which was disclosed.

- Recorded images must not be made more widely available. If it is intended that they will be made more widely available that decision must be made by the designated member of staff responsible for the scheme, and the reason for the decision must be documented.
- Where images have been disclosed to a third party, then they become the Data Controller for their copy/ies of the image/s and are responsible for compliance with the GDPR
- If images are to be disclosed to the media the images of individuals must be disguised or blurred to ensure that they cannot be readily identified. If the system does not have the facilities for this kind of editing a third party or company can be used. In such cases, the responsible member of staff must ensure that.

  - There is a contractual relationship between the Data Controller and the third party or company
  - The third party or company has given appropriate guarantees regarding security measures they take
  - The Data Controller has checked to ensure that those guarantees are met
  - The written contract makes it explicit that the third party or company can only use the images in accordance with the instructions of the Data Controller or designated member of staff.
  - The written contract makes the third part or company's security guarantees explicit.

14.1 The General Data Protection Regulation 2018 requires a Data Controller who is processing personal information to register with the Information Commissioner as Data Controller, unless they are exempt from the requirement to do so.

14.2 Northumberland County Council is registered on the Public Register of Data Controllers with the registration number Z1727733. The registration must be renewed annually. Failure to notify the Information Commissioner is a criminal offence under the General Data Protection Regulation 2018.

14.3 There is a requirement that any changes to the Council's registration must be made within 28 days. Failure to notify the Information Commissioner is a criminal offence.

14.4 The designated Manager of the CCTV system must liaise with the Council's Information Governance Office so as to enable the appropriate notification to be made.

15. Access to Recorded Images by Data Subjects

15.1 All staff involved in operating the equipment must be able to recognise a request from a member of the public for access to recorded images by data subjects.

15.2 Data subjects must be provided with a standard subject access request form which will:

- Indicate the information required in order to locate the relevant images.
- Indicate the information required in order to identify the person making the request. If the data subject is unknown to the equipment user a photograph of the individual may be requested in order to locate the correct image.
- Indicate that a fee of £10 will be charged for carrying out the search.
- Ask whether the individual would be satisfied with merely viewing the images.
- Indicate that the response will be provided promptly and in any event within 40 days of receiving the required fee and information.
- Explains the rights provided by the General Data Protection Regulation 2018

15.3 All subject access requests must be dealt with by the designated Manager of the CCTV system, who must also locate the images requested. S/he must also determine whether disclosure to the individual would entail disclosing images of third parties, and whether those third party images are held under a "duty of confidence". For example, members of the public whose images have been recorded in a town centre or streets are seen to have less expectation that their images are held under a Duty of Confidence than individuals whose images have been recorded in more private space such as a doctor's waiting room.

15.4 If third party images are not to be disclosed the responsible Manager of the CCTV system must arrange for the third party images to be disguised or blurred. If the system does not have the facilities for this kind of editing a third party or company can be used. In such cases, the designated Manager of the CCTV system must ensure that:

- There is a contractual relationship between the Data Controller and the third party or company.
- The third party or company has given appropriate guarantees regarding security measures they take.
- The Data Controller has checked to ensure that those guarantees are met.
- The written contract makes it explicit that the third party or company can only use the images in accordance with the instructions of the responsible member of staff.
- The written contract makes the third party or company's security guarantees explicit.

15.5 If the responsible member of staff decides that a subject request is to be denied, the following information must be logged:

- The identity of the individual making the request.
- The date of the request.
- The reason for refusing to supply the requested images.
- The name and signature of the manager or designated Manager of the CCTV system making the decision.

15.6 If there is any doubt about whether images are to be disclosed the Data Protection Officer and Legal Services must be consulted.

15.7 It should also be noted that in addition to requesting the disclosure of images, individuals also have the right to request notifying Northumberland County Council in writing to cease or to not begin processing images containing Personal Data likely to cause "substantial and unwarranted damage or distress. Advice can be sought from the Data Protection Officer and Legal Services.

16. Compliance

16.1 Information Security will regularly assess for compliance against this policy. Compliance with this policy is a term and condition of employment. Failure to comply with corporate policies is a potential disciplinary matter which may result in withdrawal of your access to corporate systems and disciplinary action up to and including dismissal.

17. Monitoring and Review

17.1 Monitoring for changes of ISO 27001 and this Policy is the responsibility of the Data Protection Officer, who will ensure on-going monitoring and audit of the processes / guidance in place under the policy.

17.2 Changes to the attached guidance documents are the responsibility of the Data Protection Officer but will be dependent on, for example, changes in; technology, local procedure, legislation and Northumberland County Councils computer/network infrastructure.

17.3 The Chief Information Officer is responsible for monitoring the implementation and impact of this policy.

.

18. Monitoring the Workforce (Appendix 1)

18.1 In addition to the above Policy, the following points must be addressed when considering a CCTV scheme in the workplace, whether or not the scheme is specifically designed to capture images of workers.

- A CCTV scheme installed on work premises to prevent and detect crime must not be used to monitor work done, or compliance with policies or procedures. Images should therefore only be viewed when there is suspected criminal activity.
- Cameras should be sited to avoid being directed specifically to capture images of workers.
- Images of workers should only be used if something is seen which cannot be ignored – criminal activity, gross misconduct or behaviour which puts others at risk.
- If images are used in disciplinary proceedings the footage should be retained so that workers can see it and respond, as still images may not be enough.
- If considering installation of a CCTV scheme specifically for workforce monitoring the decision-making process identified in this CCTV Policy must be followed to decide whether it is justified – in particular, consideration should be given to whether better training or greater supervision would be more appropriate.
- Such CCTV must be limited to areas where workers would not expect to be private. Cameras should not be used in toilet areas or private offices.
- Workers must be made aware that the CCTV scheme is for staff monitoring and how it will be used.
- If CCTV is used to enforce internal policies, workers must be fully aware of the policies and have received appropriate training.
- Workers have the right to submit Subject Access Requests to access images recorded of them.
- While workers should normally be aware that they are being monitored, covert monitoring can take place:

    - In an exceptional circumstance with reason to suspect criminal activity or equivalent malpractice
    - If cameras are used only for a specific investigation and removed once the investigation is complete.
    - If the investigation would be prejudiced if workers knew that cameras were being used,
    - If full account is taken of potential intrusion on innocent workers.
    - If the decision to carry out the surveillance is taken by senior management.

18.2 If a covert camera installed for one investigation reveals evidence of other criminal behaviour or disciplinary offences, such evidence can only be used where the offence is serious, such as gross misconduct or misconduct putting others at risk.

18.3 Note that any monitoring of the workforce must also comply with the Information Commissioner's Employment Practices Code.

19. Implementation

19.1 This procedure is effective immediately.

20. Monitoring and Review

20.1 This policy will be monitored by the Digital Northumberland Board and will be reviewed every two years or where there are changes to Legislation.

21. Useful Contacts

The Data Protection Officer via informationgovernance@northumberland.gov.uk

The Information Commissioner's Office via www.ico.org.uk

.