CCTV (Closed Circuit Television) Policy

March 2024

Version 1.0

Document Control Sheet

Title	CCTV (Closed Circuit Television) Policy					
Author	Information Governance Team					
Consultees	Economic Growth & Development Educational Estates Education, Resources and Communities Equalities Estates and Property Services Information Assurance Group					
Distribution	Council wide upon approval					
Version	v1.0					
Date	Mar 2024					

Contents

Definitions:

CCTV/CCTV Systems: Closed Circuit Television (CCTV) is a closed system consisting of video cameras, display devices (monitors) and wired or wireless data networks that allow the transfer of images from video cameras to monitors. There may be the capability for captured images to be recorded.

Data Controller: A body that determines the purposes and means of the processing of personal data. A data controller can act either jointly or alone. The Council is considered to be the data controller for most of its activities that involve personal data.

Data Processor: A body that processes personal data on behalf of and as specified by the data controller. Data Controllers must have a contract in place with all Data Processors they utilise (known as Data Processing Agreements).

Data Protection Legislation: means as applicable, the Data Protection Act (DPA) 2018, the United Kingdom General Data Protection Regulation (**UK GDPR**) (as defined in the DPA 2018) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, and, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any other applicable laws and regulations relating to the privacy or the processing of personal data, including any amendments or successor laws or regulations thereto. It also includes if applicable, legally binding guidance and codes of practice issued by the Information Commissioner.

Data Subject: An identified or identifiable living individual to whom personal data relates.

Data Subject Rights: Rights belonging to data subjects under data protection legislation namely: •the right to be informed •the right of access •the right to object •the right to erasure •the right to restriction of processing •the right to rectification •the right to file a complaint •the right to damages •the right to data portability, and, •rights relating to automated decision making and profiling.

Personal Data: Information relating to an identified or identifiable natural person (data subject) who: can be identified or who is identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information; such as: a name, an identification number, location data, an online identifier; or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data may also include special categories of personal data or criminal offence data.

Special Category Data: Personal data that reveals:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life;
- data concerning a person's sexual orientation.

Criminal Offence Data: Personal data relating to criminal convictions and offences or related security measures. This includes data about offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings.

Processing: Any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection Impact Assessment (DPIA): A DPIA is a process designed to help systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of accountability obligations under the UK GDPR, and helps demonstrates compliance with data protection obligations.

Privacy Notice: A Privacy Notice is required to clearly inform Data Subjects on what will happen to the personal data once collected for a set process. Privacy Notices for the Council are produced by the Information Governance Team.

Central Register of CCTV Cameras (CCTV Register): A central register of CCTV cameras will be maintained by Property Services

1. Introduction

1.1 The Council uses Closed Circuit Television (CCTV) in a range of spaces, including public spaces, Council buildings and properties, and, schools.

1.2 This document sets out the Council's policy on the use of CCTV systems to ensure that the Council acts appropriately when gathering, storing and sharing information from the use of these systems. It also aims to maintain public confidence in the use of CCTV by striking the right balance between the expectation of privacy by people going about their ordinary business, even in a public space, and, the public interests being served by the systems.

1.3 Further guidance must be produced by relevant services when they are responsible for the operation of a CCTV system, such as detailed operating procedures. Operating procedures will provide practical information on how CCTV is to be used in each area. These procedures should include, as necessary, roles and responsibilities for each system, assessments and processes to be carried out for siting of cameras, training and training records for operators, procedures for use, review records of camera siting and usage, partnership arrangements (as required), and, processes for retention and access to CCTV. Operating procedures as well as camera siting and usage should be reviewed annually to ensure they remain relevant and fit for purpose.

1.4 This Policy relates to the installation, use and management of CCTV equipment, the gathering and storage of recorded data, and, data disposal/transfer. This Policy applies to all Moray Council employees and all third party providers acting on behalf of the Council.

1.5 For the purposes of this policy, CCTV means the gathering of:

- images of individuals or people.
  This is regardless of whether this was the intended primary purpose of the CCTV. It should be noted that this includes images of Council employees as well as members of the public, even if the systems only capture images from within Council premises or land.
- images containing information that when combined with other information could identify individuals, such as an individual driving a vehicle and the vehicle's registration number plate.

1.6 This Policy does not cover:

- the capture of audio by CCTV; no audio will be captured by the Council's CCTV systems.
- the use of equipment as part of any covert surveillance operation that has been authorised in terms of the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) as these operations are subject to a separate procedure.
  Note:- CCTV systems cannot be used covertly or used for monitoring a specific individual or individuals (directed Surveillance) without specific authorisation under RIPSA. All CCTV operators must be trained in the requirements of RIPSA so that they are aware of when authorisation would be necessary.

1.7 This Policy should be read in conjunction with other Council Policies, including on Data Protection and Information Security, and any related procedures, instructions or guidance issued by the Council in connection with those policies. Whilst it is the ultimate responsibility of the Council to ensure compliance with data protection matters, in line with those policies, the relevant service is responsible for ensuring that the use of their CCTV complies with the operational requirements of this policy.

1.8 This policy should also be read in conjunction with the associated operating procedures issued by the relevant service and any failure to comply with these documents could result in serious consequences for members of the public, individual employees and the Council.

2. Purpose of CCTV Systems

2.1 It is important that all employees and especially those charged with operating CCTV systems on behalf of the Council understand exactly why each of the systems have been introduced and what the cameras will, and will not, be used for.

2.2 CCTV will be used for the following purposes:

- promoting and supporting community safety
- preventing and detecting crime
- protecting Council property and assets
- creating and supporting a safe environment for employees and the public within Council properties and in public areas
- combating and reducing anti-social behaviour
- traffic management.

2.3 New or additional purposes will be reviewed on a case-by-case basis, as and when a new need arises. In such instances, the relevant Data Protection Impact Assessment (DPIA) would require updating, in addition to, the register of cameras.

3. Legislation and Guidance

3.1 The Council recognises its legal obligations in operating CCTV systems and the rights and freedoms of individuals whose images may be captured by these systems. Images captured by CCTV systems are personal data and must be handled and used by the Council in accordance with data protection and human rights legislation. The Council is committed to operating CCTV systems in compliance with these legal frameworks.

3.2 In addition to Council Policies and procedures, CCTV operation and use are subject to legislative obligations, such as under:

- Data Protection Legislation, including:
  - The Data Protection Act 2018 (DPA)
  - The UK General Data Protection Regulation (UK GDPR)
- The Human Rights Act 1998 (HRA) in particular Article 8 (the right to respect for private and family life) provides that; (1) everyone has the right to respect for his private and family life, his home and his correspondence and (2) there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
- Freedom of Information (Scotland) Act 2002
- The Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA)

Consideration must be given as to whether the use of CCTV is necessary, proportionate and in compliance with legislative requirements, in both its application and purpose.

3.3 The Council will comply with the Scottish Government's National Strategy for Public Space CCTV in Scotland (2011) that sets out a common set of principles that owners and operators of

public space CCTV systems in Scotland should follow to ensure that these systems are operated lawfully and fairly.

3.4 The Information Commissioner's Office (ICO) regulates compliance with UK Data Protection legislation. The Council is registered with the ICO. They have produced Guidance on Video Surveillance (2022).

3.5 To ensure that CCTV systems are operating in an appropriate manner, in compliance with data protection legislation and that all practices and procedures are relevant, the Council reviews all CCTV documentation on a regular basis. It is good practice for services to review CCTV documentation annually.

3.5.1 To ensure compliance with this policy, the ICO and data protection legislation, services should review all operating procedures annually. This includes a review of all camera siting and usage determining if a camera is still needed, staff procedures are correct and whether the relevant DPIA should be updated with any significant changes.

4. Principles

4.1 The Council will comply with the following principles when installing and operating CCTV:

4.1.1 CCTV systems will only be installed and operated when there is a clearly identified need and a legal basis for their use. The processing must be necessary and proportionate. Evidence of this will be gathered, reviewed and retained for future audit and reference.

4.1.2 Data protection by design and by default will be a key consideration when new CCTV systems are acquired, or changes introduced to current systems.

4.1.3 A Data Protection Impact Assessment (DPIA) must be completed by services, and, approved before CCTV systems can be installed and operated.

4.1.4 Services must have operational procedures in place prior to utilising any new CCTV systems. All CCTV systems will be operated in accordance with documented operational procedures in which responsibilities will be clear, and effectively communicated to all relevant employees.

4.1.5 The location of CCTV systems must ensure that only necessary areas are captured by CCTV, to minimise the capture of areas not relevant to the purposes of the CCTV installation, for example private homes, neighbouring properties and areas where staff are working (where possible).

4.1.6 CCTV systems will not record audio.

4.1.7 CCTV systems will only capture images of a suitable quality for the purposes for which the systems have been installed.

4.1.8 The Council has an obligation under data protection legislation to process personal data securely by means of appropriate technical and organisational measures. Services will ensure that controls are implemented to restrict access and use of captured images to authorised personnel only.

4.1.9 Clear signage will be put in place to inform individuals that they are in an area where CCTV is in operation, with a link to a Privacy Notice available on the Council's website.

4.1.10 Measures should be put in place to protect CCTV systems from vandalism.

4.1.11 All images captured will be retained for the minimum amount of time necessary for the purpose(s) that the CCTV systems have been installed for, and, comply with the Council's Retention Schedules. Service operating procedures should clearly specify the particular retention cycles applicable to each CCTV system.

5. Responsibilities – Existing Systems

5.1 A DPIA is required for each process that collects personal data. This is required before any personal data is collected and is a method by which the Council demonstrates it is aware of, and complying with, its data protection obligations. A DPIA is needed per collection process; a collection process may cover more than one physical camera or location.

5.2 Retrospective DPIAs are required for existing CCTV systems. It is the responsibility of the service responsible for the operation of a system to undertake a DPIA and to record the matters considered in it and what steps have been taken to minimise intrusion into the private lives of individuals. This DPIA must be retained, kept up to date and made available if required.

5.3 Each service shall provide, on completion of each DPIA or sooner, the appropriate details to be included within the CCTV Register in relation to ongoing CCTV systems at the commencement of this Policy.

5.4 All CCTV systems owned by Moray Council, or its partners, such as within the Public Private Partnerships (PPP), will require an Information Sharing Protocol or Data Processing/Sharing Agreement. These agreements will also confirm the maintenance regime including an annual inspection and service visits.

5.5 In relation to the use of CCTV overtly in a public space, and which would capture images of individuals, to ensure that individuals are aware that they are entering an area where CCTV systems are in operation, signage will be displayed at the entrance and within the controlled area advising that surveillance cameras are in operation.

5.6 Employees of Moray Council involved in the operation of CCTV systems will undertake the necessary training detailed within the service operating procedures. All training within service operating procedures should also include training on the HRA with regard to Article 8 in particular and the requirements of RIPSA. Services must ensure training is completed prior to operating the CCTV systems and that training records are maintained.

5.7 On the commissioning of any new camera or CCTV system, the service responsible for that camera or system shall, without delay, advise the Property Helpdesk of the appropriate information to be included in the CCTV Register.

6. Central Register of CCTV Systems

6.1 In order to assist it to meet its legal obligations in relation to CCTV, the Council will maintain a Central Register in relation to the systems of CCTV that are in commission in terms of this Policy.

6.2 This register shall be maintained by Property Services, specifically by the Asset Manager (Corporate Buildings), via the Property Helpdesk (PropertyHelpdesk@moray.gov.uk), and shall include;

- details of the service responsible for the use of that camera,
- the location of each CCTV camera/system operated by the Council (storage location in relation to any mobile CCTV systems),
- the purpose for each of the cameras being used,
- a link to the signed off DPIA for that process, ~~and~~
- a link to the relevant Privacy Notice, and,
- the owner of the CCTV system; Council, external (e.g. PPP)

7. Information Management

7.1 Moray Council will, in so far as possible, ensure that all recorded data gathered by CCTV systems, which are under its control whether operated by the Council or on the Council's behalf, is securely stored and used only in accordance with the terms of the relevant legislation, and, in accordance with Council policy and guidelines.

7.2 Information Sharing Protocols, Data Sharing Agreements or Data Processing Agreements should be agreed with all third parties, such as Public Private Partnerships (PPP), Police Scotland and other such parties.

7.3 CCTV systems installed within facilities operated on behalf of the Council by third party service providers will use Moray Council policies and procedures for the management of CCTV systems.

7.4 CCTV systems installed by third parties, such as PPP within the PPP Schools estate will use a common data management process that matches the Council process in relation to retention periods, data security and the sharing of CCTV information.

7.4. The Council's CCTV webpage provides transparency and clarity regarding the Council's use of CCTV. It should be kept up-to-date with any relevant changes: www.moray.gov.uk/CCTV

8. Operational Use of CCTV Systems

8.1 All employees involved in the operational use of CCTV systems will use the equipment in accordance with the terms of the relevant legislation and in accordance with Council policies and procedures.

8.2 The Council will maintain appropriate policies and procedures relating to the use and management of CCTV systems.

8.3 Services should ensure that all involved in the operational use of CCTV systems will be trained to a standard appropriate to their use of the specific system under their control. Training will be outlined within the service operational procedures. Training should be completed prior to using the CCTV system.

8.4 CCTV systems set up to protect Council properties and other related purposes will be configured to match the operational needs of the individual sites and will not be used in any way that does not comply with this Policy.

8.5 It is important that CCTV systems are monitored in relation to the adequacy of the images that are gathered in relation to its specified purposes. If the information gathered is inadequate for its purposes then the system must not be used to gather information to which this Policy relates.

9. Installation of new CCTV systems and extension of existing systems

9.1 The Council is committed to respecting people's rights to privacy and supports the individual's entitlement to go about their lawful business. This is a primary consideration in the operation of any CCTV system. However, this must be balanced against the public interest of the Council in relation to installing or extending existing CCTV systems. Covert CCTV will not be installed unless it is appropriately authorised through RIPSA.

9.2 The Council will not consider the installation or extension of a CCTV system as an automatic step to address a problem and will always consider less privacy intrusive solutions. CCTV will only be used if it is deemed proportionate and appropriate. The issues of interference with privacy, including necessity and proportionality of that interference must be recorded in the DPIA. Existing DPIAs will need to be updated to cover any significant changes including a proposed extension to the CCTV system.

9.3 The service responsible for the initiative will complete a DPIA and involve the Asset Manager (Corporate Buildings) in the process.

9.4 The Council does not encourage the use of "Dummy" or "Replica" cameras, as these give a false sense of security.

10. Review, sharing and transfer of CCTV data

10.1 No images captured by the Council's CCTV systems will be disclosed to any third party, unless there is a lawful basis to do so. Requests regarding the transfer of CCTV data will be handled on a case by case basis. Relevant Data Sharing Agreements (DSA) should be in place, or, relevant Data Protection Request Forms will be required before any information may be shared to a third party.

10.2 Services will retain detailed records of the following when disclosing captured images to third parties:

- date and time at which access was allowed;
- identification of any third party who was allowed access;
- reasons for allowing access; and
- details of the captured images to which access was allowed.

A Disclosure Request Form must be completed by the third party.

10.3 Only employees that have been authorised and completed the appropriate training, will be involved in the review and sharing of CCTV data.

10.4 In order to meet the public interests in using CCTV, it may be appropriate for the Council to transfer information gathered by CCTV to other third parties on reviewing the information gathered without the necessity of the third party making a formal request to obtain a copy of the information, for instance in a case of urgency or where any delay would be contrary to the public interest. Such transfers shall only be made where permitted in terms of legislation and relevant Council policies and procedures. Services should record if CCTV data has been shared, with whom and for what purpose.

10.5 Any person who misuses, misplaces, makes unauthorised copies or transfers recorded CCTV data to a third party for purposes not related to Council or lawful purposes could be liable to disciplinary and/or criminal proceedings.

11. Individual requests for access to or erasure of captured images

11.1 Data Protection legislation grants rights to individuals in relation to their personal data. This includes rights to request access to, and erasure of, personal information, such as images captured by CCTV. Access to Information requests, including Subject Access Requests, Freedom of Information (Scotland) Act Requests and Environmental Information (Scotland) Regulations Requests are coordinated through info@moray.gov.uk

11.2 The Council retains copyright in all images captured by its CCTV systems. Any further use or publication of images provided to an individual in response to an Access to Information Request is prohibited, unless the individual obtains authorisation from the Council.

11.3 The Council is entitled to refuse access to captured images in limited circumstances, such as where disclosure would prejudice the prevention or detection of crime or the prosecution of offenders. Where captured images have been passed to Police Scotland or the Crown Office and Procurator Fiscal Service, a Subject Access Request from an individual will be refused until such time as the Council has been notified that no proceedings will be taken, or proceedings have concluded.

11.4 Subject Access Requests for images on Public Space CCTV must be made directly to Police Scotland, as they monitor and operate the CCTV system.

12. Review of Systems

13.1 All operating CCTV systems shall be reviewed by services on an annual basis to ensure that the justification for their use remains.

13.2 The images captured by CCTV systems shall be reviewed on a periodic basis as set out in the service operating procedures to ensure that they are still adequate and effective in relation to meeting the purposes of the system.

13. Joint systems

13.1 There may be situations where the Council is operating a CCTV system with a third party. This would usually occur where the premises to which the systems relate are operated as a shared or communal facility. In those cases, the Council will not use the images from such a system unless that use complies with the requirements of this Policy, even if the system was not implemented by the Council.

13.2 The Council and the third party should put in place joint operational measures in order to ensure that the Council's use of the CCTV system and the images captured complies with legislation and this Policy.

14. Complaints

14.1 Any complaints will be recorded and handled in accordance with the Council's formal complaints procedure, relevant services will provide assistance as and when required.

15. Privacy Notices and Signage

15.1 Privacy Notices should be made available to potential data subjects and should be kept up-to-date: www.moray.gov.uk/PrivacyNotices

15.2 The CCTV Privacy Notice will be clearly accessible from the Council's CCTV webpage, this webpage should be included on all Council CCTV Signage.

15.3 All CCTV Signage needs to be clearly and prominently placed at the entrance and also within the CCTV coverage area.

15.4 All CCTV Signage should contain layered privacy information, including naming the Data Controller, the purpose(s) for using the CCTV, where further data protection information can be found including a link to the full Privacy Notice, and, contact details for further information.

16. Further Information

Moray Council's CCTV webpage: www.moray.gov.uk/CCTV

ICO Guidance on Video Surveillance, including CCTV version 1.0 (2022)
https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv-1-0.pdf

Scottish Government's National Strategy for Public Space CCTV in Scotland (2011)
https://www.gov.scot/binaries/content/documents/govscot/publications/advice-and-guidance/2011/03/national-strategy-public-space-cctv-scotland/documents/0115210-pdf/0115210-pdf/govscot%3Adocument/0115210.pdf