CCTV Operation and Information Management Policy

For more information or if you want this information in a different format or language, please phone 0303 123 1015 or email equalities@southlanarkshire.gov.uk

South Lanarkshire Council
CCTV Policy

1. Introduction

1.1 The Council uses Closed Circuit Television (CCTV) in public spaces, properties, vehicles and body worn systems. It also uses CCTV for building inspection uses.

1.2 This document along with the associated operating procedures to be issued by the Executive Director of the Resource which is responsible for the operation of such CCTV sets out the Council's policy on the use of CCTV systems to ensure that the Council acts appropriately when gathering 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 This Policy relates to the installation and use of CCTV equipment, the gathering and storage of recorded data and its disposal/transfer. This Policy applies to all employees employed by South Lanarkshire Council and is the standard expected from facilities management employees using CCTV systems installed within the Public-Private Partnership (PPP) secondary schools estate and within temporary accommodation facilities operated on behalf of the Council by third party providers.

1.4 For the purposes of this policy, CCTV means the gathering of images of

- people or individuals by the Council regardless of whether that was the intended primary purpose of the CCTV and includes systems which also record sound as well as images. 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. It does not apply to 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 as these operations are subject to a separate procedure.
- images that contain information that when combined with other information can identify individuals such as Automatic Number Plate Recognition

1.5 The CCTV Policy should be read in conjunction with other Council Policies, including its Privacy Policy, Information Security Policy and Data Sharing Policy (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 Executive Director for each of the Resources is responsible for ensuring that the use of CCTV cameras by that Resource complies with the operational requirements of this policy.

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

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 by South Lanarkshire for the following purposes;

- promoting and supporting community Safety
- preventing and detecting crime
- protecting council property assets

- creating and supporting a safe environment for employees and public within SLC properties and in public areas where the Council is carrying out operations
- combating and reducing anti social behaviour
- traffic management and building inspection

2.3 The systems will not be used for any other purpose or purposes unless compatible with the law. An additional purpose could be meeting other legitimate interests of the Council or any other persons where sharing is justified and necessary (including proportionate) but only where to do so would comply with the requirements of the Data Protection Act 1998 and on an ad hoc basis and not systematic data sharing as set out in the Council's Data Sharing Policy.

3. Legislation / Guidance

3.1 In addition to Council Policies, procedures and operational guidelines CCTV operation and use are subject to legislation under:
- The Data Protection Act 1998 (DPA)
- The General Data Protection Regulation (the GDPR) (which comes into effect on 25 May 2018)
- The Human Rights Act 1998 (HRA)
- Security Industry Act 2001.

3.2 The Council will also comply with the Scottish Government's CCTV Strategy for Scotland.

3.3 To ensure that CCTV systems are operating in an appropriate manner and in compliance with legislation, the Council review all CCTV documentation bi-annually (or as legislative changes occur) to ensure that all practices and procedures are relevant.

4. Responsibilities – Existing systems

4.1 The Council appreciates that this Code of Practice reflects its legal obligations as they currently stand and so this policy will be applied retrospectively to existing systems. The Council does not require the undertaking of any PIAs in respect of existing systems. However, if an existing system collects images of identifiable individuals (regardless of whether the person is identifiable to the Council by name), such systems must be assessed in relation to information that is being collected by them. This assessment would be
- a statement as to the purposes of the processing (including identifying what condition or conditions are met in Schedule 2 (and where the processing involves sensitive personal data, condition or conditions in Schedule 3) of the Data Protection Act 1998 i.e. the processing would be the collection of images or the relevant conditions in place after the implementation of the GDPR from 25 May 2018
- an assessment of the necessity and proportionality of the processing in relation to those purposes (which would generally be an explanation as to how the identified condition or conditions in Schedule 2 (and 3, where appropriate) or the relevant conditions in place after the implementation of the GDPR from 25 May 2018 is met)
- assessment of the risks to the rights and freedoms of all data subjects whose personal data/sensitive personal data/special category data (under the GDPR) is to be processed (this would include the risks to any of the individuals (whose personal data/sensitive personal data/special category data would be processed) of harm, physical or financial and distress caused by the Council carrying out the processing in contravention of any of the data protection principles as set down by the DPA and those set down by the GDPR) and the measures that have been put in place to address those risks, including safeguards (both technological and organisational) and mechanisms to ensure the protection of the personal data/sensitive personal data and to demonstrate compliance with the data protection principles taking into account the rights and legitimate interests of the people whose personal data is to be processed and other persons concerned.

4.2 It shall be the responsibility of the Resource responsible for the operation of the existing system to undertake this assessment and to record the matters considered in it and what steps have been taken to minimise intrusion into the private lives of individuals. This

assessment must be retained and made available if required. It will not be recorded as a PIA in terms of the Council's procedures.

4.3 Each Resource shall provide, on completion of each assessment or sooner, the appropriate details to be included within the Central Register of CCTV Cameras (see Section 7) in relation to ongoing CCTV systems at the commencement of this policy.

5. Responsibilities - Before operation of a new CCTV system

5.1 Before operating a new CCTV system (including any extension to the current systems by the erection of new cameras or the relocation of existing cameras) the Council must carry out a Privacy Impact Assessment (PIA) as required in terms of Council Policy. This PIA must include the following

- the purposes of the processing (including identifying what condition or conditions are met in Schedule 2 (and where the processing involves sensitive personal data, condition or conditions in Schedule 3) of the Data Protection Act 1998 or the relevant conditions in place after the implementation of the GDPR from 25 May 2018
- an assessment of the necessity and proportionality of the processing in relation to those purposes (which would generally be an explanation as to how the identified condition or conditions in Schedule 2 (and 3, where appropriate) or the relevant conditions in place after the implementation of the GDPR from 25 May 2018 is met)
- assessment of the risks to the rights and freedoms of all data subjects whose personal data/sensitive personal data is to be processed (this would include the risks to any of the individuals (whose personal data/sensitive personal data would be processed) of harm, physical or financial and distress caused by the Council carrying out the processing in contravention of any of the data protection principles) and
- the measures that are to be put in place to address those risks, including safeguards (both technological and organisational) and mechanisms to ensure the protection of the personal data/sensitive personal data and to demonstrate compliance with the data protection principles taking into account the rights and legitimate interests of the people whose personal data is to be processed and other persons concerned.

5.2 Consequently, before setting up any new cameras, it is important to be sure that the purpose behind the CCTV cameras is recorded and that there is an assessment of the information that will be caught by the system. There must be as little as possible collateral intrusion into the private lives of people. For instance, extreme care must be taken if the images were to catch identifiable people entering and leaving a doctor's surgery.

5.3 South Lanarkshire Council will ensure that all data retention periods are appropriate to the use and purpose of individual CCTV systems and will outline them in the relevant Operational Guidelines documentation. The determination of the relevant retention period must be set prior to the installation and use of a CCTV system (and as such form part of the PIA). The setting of the relevant retention period will depend upon the purpose of the system (as set out in paragraph 2.2 previously) and the Resource responsible for gathering the information will be responsible for setting appropriate retention periods. Once there is no longer a business case for retaining CCTV images as set by the retention period, all images must be destroyed securely.

6. Responsibilities – Commencing the operation of a new CCTV system

6.1 All CCTV systems owned by South Lanarkshire Council and its partners within the PPP will be subject to a maintenance regime including an annual inspection and service visits.

6.2 In relation to the use of CCTV overtly in a public place and which would capture images of them, to ensure that people are aware that they are entering an area where CCTV systems are in operation signage will be displayed advising that surveillance cameras are in operation. Examples of the signage used can be found at Appendix 'A'

6.3 Employees of South Lanarkshire Council involved in the operation of CCTV systems for the surveillance of public spaces will be trained to standard approved by the Security Industry Authority.

6.5 On the commissioning of any new camera or CCTV system, the Resource responsible for that camera or system shall, without delay, advise the Security Manager of the appropriate information to be included within the Central Register of CCTV Cameras (see Section 7)

7. Central Register of systems

7.1 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.

7.2 This register shall be maintained by the Security Manager and shall include

- details of the Resource responsible for the use of that camera
- the location of each CCTV camera operated by the Council (except in relation to any mobile CCTV systems)
- the purpose for each of the cameras being used as detailed in paragraph 2.2 and
- a statement that an assessment or a PIA as necessary has been undertaken in respect of that camera.

8. Data management

8.1 South Lanarkshire Council will ensure that all recorded data gathered by CCTV systems, which are under its control whether operated by the Council or others, is securely stored and used only in accordance with the terms of the relevant legislation and in accordance with Council policy and guidelines.

8.2 With the exception of Council owned body worn CCTV systems a common Council wide data management process will be used which makes best use of available technology and the Council's Wide Area IT Network.

8.3 Council owned body worn CCTV systems will operate a common data management process with recorded data being retained securely at the main operational office of the responsible Resource.

8.4 CCTV systems installed within temporary accommodation facilities operated on behalf of the Council by third party service providers will use South Lanarkshire Council operational guidelines for the management of CCTV systems.

8.5 CCTV systems installed within the PPP Secondary Schools estate will use a common data management process which matches the Council process in relation to retention periods, data security and the sharing of CCTV information.

9. Operational use of CCTV systems

9.1 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 the Council policy and guidelines.

9.2 The Council will maintain appropriate operational guidelines relating to the use and management of CCTV systems.

9.3 All employees 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.

9.4 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.

9.5 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.

9.5 Any person involved in the operational use of CCTV systems installed within the PPP. Secondary Schools estate and within temporary accommodation facilities will be trained to a standard appropriate for their use of the systems.

10. Installation of new CCTV systems and the extension of existing systems

10.1 South Lanarkshire 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 the system.

10.2 The Resource sponsoring the initiative will involve the Security Manager in the process and work in conjunction to complete a Privacy Impact Assessment (PIA). This PIA will be carried out and contain the matters and considerations required by the Council and set down in the relevant Guidance.

10.3 South Lanarkshire Council will not consider the installation 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 set out in the report from the PIA. It must be accepted that there will inevitably be some loss of privacy when CCTV systems installed but that this must be justified by the Council. Any PIA must take account of the sensitivity of the personal data obtained through CCTV and the expectations of the people whose personal data is being gathered.

10.4 South Lanarkshire Council will not deploy "Dummy/Replica" cameras as these give a false sense of security.

11. South Lanarkshire Council video sentry re-deployable CCTV systems

11.1 South Lanarkshire Council owns and operates a bespoke re-deployable CCTV camera system which is capable of being linked into the South Lanarkshire Council CCTV Control Centre for proactive monitoring and the system is managed by the Council's Anti-Social Investigation Team.

11.2 As well as complying with the requirements of the Council in relation to the general installation of or the extension of any new CCTV, the background information supporting a request for the installation of a Video Sentry CCTV Camera system is gathered via the South Lanarkshire Council's Problem Solving structure with deployments being carried out for a fixed period of 3 months.

11.3 No deployment will extend beyond 3 months without the extension being formally considered in accordance with the operational guidelines governing the use of the Video Sentry Re-deployable CCTV Camera system.

12. Review and transfer of CCTV data

12.1 The review and transfer of CCTV data will be subject to a standard Council wide process which will apply to all CCTV systems owned and operated by South Lanarkshire Council.

12.2 All employees with access to recordings made from CCTV must do so and use the information in connection with the Council's functions. They must keep such information confidential and securely in line with the relevant Council policies. Only employees that have been authorised,

having completed the appropriate training, will be involved in the review and sharing of CCTV data.

12.3 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 bodies on reviewing the information gathered without the necessity of the other body 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 be only be made where permitted in terms of legislation and relevant Council policies and procedures.

12.4 Such transfers of data from property CCTV systems for Council or Policing purposes will be governed by a centralised process and only be made by employees who have been specifically authorised by the Council to do so.

12.5 All reviews of recorded CCTV data carried out for Council or Policing purposes will be logged on a central register.

12.6 All occasions where recorded CCTV data is transferred or copied for Council or Policing purposes will be logged on a central register.

12.7 Any person who misuses, misplaces, makes unauthorised copies or transfers recorded CCTV data to another person/organisation for purposes not related to Council or Policing purposes could be liable to disciplinary and/or criminal proceedings.

12.8 All records relating to the review and sharing of recorded CCTV for Council or Policing purposes will be retained in accordance with the relevant Council policy and guidelines.

13. Sharing of CCTV information on request

13.1 The sharing of recorded CCTV data with internal and external partners is acceptable in the following circumstances;

- Community Safety and Policing
- Health and Safety
- Environmental and licensing
- Public and employee liability
- If necessary to meet a statutory or public function of or the legitimate interests (but not after 25 May 2018 in relation to sharing based on legitimate interests) of the person or organisation with whom it is to be shared.

13.2 Consequently, requests for information gathered by CCTV may be requested by

(a) organisations responsible for investigation for the prevention and detection of crime or the crime or the apprehension of offenders such as Police Scotland and other public bodies discharging this sort of public task or

(b) other organisations or people seeking the CCTV information because it is necessary in order to meet their legitimate interests or some other justifiable lawful reason, including the making of a request for information in terms of either the Environmental Information (Scotland) Regulations 2004 or the Freedom of Information (Scotland) Act 2002.

13.3 Responsibility for coordinating all requests will rest with the Security Manager. The decision as to when and what information to share shall be completely at the Council's discretion (unless the sharing is required by operation of law but this does not include any obligations in terms of FOISA) and any decision as to whether to comply with the request shall be taken by the Council alone.

13.4 All requests for CCTV information will be dealt with in accordance with the relevant legislation, policies and guidelines set out by the Council. Unless required by operation of law or court order, the Council will consider each request on an individual basis.

14. Review of systems

14.1 All operating CCTV systems shall be reviewed on a periodic basis to ensure that the justification for their use still remains. This review shall consist of the review of the purpose of the system and whether its use for the gathering of images (and where relevant sound recordings) remain necessary and proportionate in respect of that purpose.

14.2 The images gathered by systems shall be reviewed on a periodic basis to ensure that they are still adequate and effective in relation to meeting the purposes of the system.

15. Joint systems

15.1 There may be situations where the Council is operating a CCTV system with another person, organisation or company. 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 but by that other party.

15.2 The Council and the other party, who are responsible for the operation of such systems, will put in place joint operational measures in order to ensure that the Council's use of the CCTV system and the images gathered by it complies with this policy and the law.

16. Subject Access Requests

16.1 The Council must comply with its obligations as a data controller as set down by the DPA and, when it comes into force the GDPR. This includes the right of a data subject to make a request for a copy of any information obtained by CCTV which relates to their personal data in terms of section 7 of the DPA (subject access request) or the equivalent right contained within the GDPR.

16.2 All such subject access requests will be dealt with in accordance with the terms of the relevant legislation and in accordance with the Council policy and guidelines.

17. Complaints

17.1 Any complaints, other than complaints which relate to rights of a person in terms of the DPA including

- the compliance with the first data protection principle (including the lawfulness and proportionality of the information gathered as a result of CCTV)
- the rights protected by the sixth data protection principle Including the making of subject access requests) and
- any information security incidents that may amount to non-compliance with the seventh data protection principle

received in relation to the operation of a CCTV system will be recorded in accordance with the Council's formal complaints procedure and coordinated by the Security Manager who will in work in conjunction with the Resource to ensure the matter is concluded appropriately. Where the incident involves the disclosure of information to which the Council's Information Security Incidents procedures apply (particularly if the information to which the complaint relates is personal data), the incident must be notified to the Council's Information Governance Board in accordance with the Council's reporting procedures.

17.2 All complaints in respect of matters which relate to the rights of the individuals and compliance with the data protection principles must be dealt with in accordance with the Council's procedures for complaints falling within this category.

18. Appropriate supporting operating procedures

18.1 It shall be the responsibility of the Executive Director for the Resource responsible for the operating of CCTV systems to issue appropriate supporting operating procedures to be followed by employees in relation to that CCTV system. These procedures shall include when to complete a PIA (including the re-assessment of systems existing prior to the implementation of this policy) in relation to new systems or the extension or changes to existing systems and the maintenance of records to show the matters considered in the assessment where this is not a formal PIA

(a) how and when to complete the Register of all CCTV recording devices including the purpose for which they are required
(b) roles and responsibilities including a list of all officers permitted/trained to be involved in the operational use of CCTV systems
(c) retention periods
(d) review periods and the matters to be reviewed in relation to the operation of the CCTV including the assessment of need for the system and the necessity and proportionality of the gathering of images
(e) training requirements and records of employees who have received this training as part of the required functions of their posts
(f) responsibility for the erection, maintenance and, where no longer required, removal of all signage
(g) appropriate security arrangements in relation to the security of and access to the images gathered
(h) the responsibility for processing all requests for the sharing of images (including sound recordings) gathered, including the processing of subject access requests and
(i) the keeping of copies of all operating procedures issued for as long as those procedures remain in force and effect in a central register for that Resource.

As approved by the Executive Committee on 8 November 2017